Sécurité de la plateforme Zurich

Dernière mise à jour: 17/12/2025

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La présente documentation a été traduite pour vous simplifier sa lecture, à l'aide d'un logiciel de traduction. Tous les efforts possibles ont été déployés pour fournir une traduction précise, toutefois, la traduction automatique ne peut en aucun cas remplacer les traducteurs humains. La traduction est fournie « en l'état ». Aucune garantie, quelle qu'elle soit, express ou implicite, n'est fournie concernant la précision, la fiabilité ou l'exactitude des traductions, quelle que soit la langue cible. En raison des limites inhérentes au logiciel de traduction, certaines traductions du contenu peuvent ne pas être exactes. La langue officielle de la présente documentation est l'anglais Toute déviation ou différence générée par la traduction ne peut en aucun cas être considérée comme juridiquement contraignante, et ne pourra avoir d'effet juridique sur la conformité ou l'application des dispositions de la documentation.

Certains des exemples et graphiques présentés ici sont fournis à des titres d'illustration uniquement.ªucune association ou connexion réelle à des produits ou services ServiceNow n'est voulue et ne devrait être inférée.

ServiceNow, le logo ServiceNow, Now et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. Les autres sociétés et noms de produits peuvent être des marques commerciales des sociétés respectives avec lesquelles ils sont associés.

Veuillez lire les Conditions d'utilisation du site Web de ServiceNow à l'adresse www.servicenow.fr/terms-of-use.html

Traduction automatique

Siège social de la société
2225 Lawson Lane
Santa Clara, CA 95054
États-Unis
(408) 501-8550

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sommaire

Sécuriser votre instance **10**

ServiceNow Coffre-fort **12**

Explorer ServiceNow Coffre-fort 13

Configurer ServiceNow Coffre-fort 16

Installer les modules d'extension 16

Utiliser la configuration guidée 17

ServiceNow Coffre-fort Tableau de bord de la console 19

Coffre-fort guidé 21

Outils et mesures 22

Sécurité de la plateforme **26**

Centre de sécurité 28

Page de destination de Centre de sécurité 30

Gestion des identités et des accès 32

Console de configurations de sécurité 33

Console de surveillance de Sécurité 68

Console de posture de sécurité 87

Tâches de sécurité 111

Apprentissage de la sécurité 117

Annonces de bannières de sécurité 118

Centre de sécurité de l'instance 119

Migration vers le centre de sécurité 128

Surveiller les événements de sécurité 131

Vérifier le score de conformité quotidien et configurer les paramètres des propriétés de sécurité 136

Rechercher des définitions de sécurité incorrectes 146

Surveiller les mesures d'instance 147

Activer l'interface ISC Agent virtuel 160

Paramètres de sécurisation renforcée 162

Versions de base de référence 163

Contrôle d'accès 255

API et service web 329

Architecture, conception et modélisation des menaces 344

Authentification 360

Logique métier 396

Communications 400

Configuration 406

Protection des données 420

Gestion et journalisation des erreurs 424

Fichiers et ressources 433

Code malveillant 442

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des sessions ... 444
Cryptographie stockée ... 462
Validation, nettoyage et codage ... 464
Service d'exportation de journal (LES) ... 503
Explorer ... 505
Administrer ... 508
Configurer ... 511
Utiliser ... 524
Référence ... 526
Journaux ... 527
Journaux système ... 528
Journalisation, audit et erreurs ... 542
Gestion des secrets ... 543
Explorer la gestion des secrets ... 544
Configuration des secrets accessibles aux clients ... 549
Tableau de bord de gestion des secrets ... 567
Signature de code ... 579
Explorer ... 583
Configurer ... 586
Utilisation de la signature de code ... 611
Tableau de bord d'intégrité et d'état ... 626
Administrer et dépanner ... 633
Analyse antivirus ... 640
Exploration de l'analyse antivirus ... 641
Configurer Analyse antivirus ... 643
Examen des fichiers en quarantaine ... 644
Examiner l'activité antivirus ... 645
Présentation des attributs du dictionnaire ... 645
Assainisseur HTML ... 647
Explorer l'assainisseur HTML ... 648
Configuration de l'assainisseur HTML ... 651
Activation de l'assainisseur HTML ... 652
Activer l'assainissement sur les champs individuels ... 652
Activer la connexion à l'assainisseur HTML ... 653
Audit ... 654
Explorer ... 655
Audit des composants ... 656
Configurer ... 659
Activer l'audit de la liste d'inclusion pour une table ... 659
Exclure un champ de l'audit (liste d'exclusion) ... 660
Inclure un champ de table dans l'audit (liste d'inclusion) ... 660
Activer l'audit pour une table système ... 661

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Console de gestion de l'audit....661
Revue....663
Fonctionnement de la table Changement de relation d'audit (sys_audit_relation)....664
Référence....664
Différences entre les ensembles d'audit et d'historique....666
Contrôler l'accès à l'historique....667
Modifier le nombre d'entrées d'historique....667
Liste de l'historique....667
Calendrier de l'historique....669
Chronologie de l'historique....671
Suivi des changements apportés aux champs de référence....675
Insertions de suivi....675
Suivi des relations CI....675
Paramètres de sécurité élevée....677
Explorer les paramètres de haute sécurité....677
Activation des paramètres de sécurité élevée....688
VPN (Virtual Private Network)....692
Explorer le réseau privé virtuel (VPN)....693
Activer un service VPN....695
Configuration d'une adresse pour la communication VPN....696
Autres paramètres et ressources de sécurité....697
[store-future: BEGIN review]
Propriétés des paramètres de sécurité....698
Guide de déploiement sécurisé du MID Server....703
Sécurité physique....704
Sécurité de l'infrastructure virtuelle....704
Sécurité du système d'exploitation....704
Sécurité réseau....705
Administrer et gérer....706
Comportement réversible....708
Remplacement sécurisé....708
Aucun remplacement de base de données....709
Propriétés de sécurité déconseillées....709
Remplacement du mode de collecte (obsolète)....709
Authentification SMTP (obsolète)....710
Utilisation de JavaScript Contrôle d'accès au contenu....710
Autres ressources de sécurisation renforcée de la sécurité....712
[End]
Confidentialité de la plateforme....713
Exploration de la confidentialité des données....714
Confidentialité des données....715
Confidentialité des données pour Now Assist....717

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confidentialité des données....719
Séparation de domaine....737
Types de champs pris en charge pour l'anonymisation....737
Rôles de confidentialité des données....739
Confidentialité des données (classique)....740
Détection de données....754
Exploration Détection de données (classique)....755
Détection de données Boutique....776
Classification des données....789
Exploration de la classification des données....790
Installation de données de démonstration du module d'extension....792
Création de classifications des données....793
Affectation de classifications de données à des entrées de dictionnaire....794
Analyse des classifications des données....795
Séparation de domaine....797
Chiffrement....799
Key Management Framework....802
Explorer le cadre de gestion des clés....803
Configuration du cadre de travail de gestion des clés....811
Référence du cadre de travail de gestion des clés....828
Actions de gestion des clés....841
Importer une clé à partir d'un service Web....844
Intégrité de Key Management Framework....847
Préparer votre instance à l'obsolescence de GlideEncrypter....848
Échange de ressources du cadre de travail de gestion des clés....853
Sécurité de l'infrastructure....860
Chiffrement Password2 avec Key Management Framework (KMF)....862
Certificats....865
Explorer les certificats....866
Génération d'un certificat client LDAP....868
Chargement d'un certificat sur une instance....870
Chiffrement de champ....871
Explorer Chiffrement de champ....873
Configurer Chiffrement de champ....875
Utiliser Chiffrement de champ....900
Chiffrement de champ Enterprise....934
Chiffrement dans le cloud avec gestion des clés....939
Opérations de gestion des clés....941
Politique de contrôle du quorum....949
Transactions de gestion des clés....953
Connexion de Chiffrement dans le cloud....955
Détection d'altération....958

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrement intégral du disque....961
Chiffrement Edge....961
Explorer Chiffrement Edge....963
Planification de Chiffrement Edge....976
Installation de Chiffrement Edge....985
Mise à niveau de Chiffrement Edge....1036
Configuration de Chiffrement Edge....1044
Chiffrement de la base de données....1101
Exploration du chiffrement de base de données....1102
Demande de rotation de clé de base de données....1104
Chiffrement de la base de données avec commutateur contrôlé par le client....1105
Gestion des accès....1107
Accès zéro confiance....1108
Explorer ZTA....1110
Activation de ZTA....1112
Configuration du rôle d'accès à la session....1112
Propriétés système....1114
Tutoriel : Utiliser ZTA....1117
ZTA pour mobile....1121
Authentification continue (CA)....1123
Domain Separation pour les fournisseurs de services....1153
Explorer la séparation de domaine....1155
Prise en charge des applications pour Domain Separation....1174
Pratiques recommandées pour les fournisseurs de services....1183
Aide de Domain Separation....1225
Configuration et administration....1226
Centre Séparation en domaines....1262
Authentification....1270
Authentification adaptative....1273
Authentification API....1338
Politique d'accès API....1351
Authentification basée sur certificat....1375
URL d'instances personnalisées....1383
Sorties d'installation....1391
Authentification basée sur la plage IP....1393
Intégration LDAP....1396
Sessions simultanées limites....1462
Authentification locale....1467
Authentification multifacteur....1493
Authentification unique (SSO) de plusieurs fournisseurs....1576
Authentification OAuth....1668
Authentification personnelle....1736

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

S’inscrire automatiquement auprès de l’instance ServiceNow 1741
Authentification basée sur un jeton (connexions de l’utilisateur) 1752
Intégrables Web 1767
Sécurité des services Web 1770
Règles de la liste de contrôles d’accès 1775
Explorer les listes de contrôle d’accès 1776
Configurer une règle ACL 1796
Gestionnaire de sécurité contextuelle 1802
Configuration avancée de l’ACL 1808
Attributs de sécurité 1820
Notions fondamentales des attributs de sécurité 1821
Créer des attributs de sécurité 1821
Périmètre de l’attribut de sécurité 1825
Requête de champ Rôles et restrictions 1825
Configurer un rôle de requête de champ 1826
Configurer les restrictions de requête de champ 1826
Outil de gouvernance de scripting 1827
Contrôles d'accès à l'identité de machine 1829
Créer un contrôle d’accès à l’identité de la machine 1829
Filtration des données 1831
Explorer la filtration des données 1832
Activer la filtration des données 1835
Créer des règles de filtration des données 1835
Créer des critères de sujet 1839
Débogage de la filtration des données 1842
Bonnes pratiques en matière de filtre de données 1844
[store-future: BEGIN review]
[End]
Filtres de données de sécurité 1844
Créer un filtre de données de sécurité 1847
Filtres de sécurité par défaut 1848
Rôles de sécurité 1849
Explicit Roles 1850
Rôles à privilèges élevés 1858
Connexions et informations d'identification 1860
Explorer les informations d’identification, les connexions et les alias 1862
Mise en route des connexions 1878
Introduction aux informations d’identification 1890
Algorithmes d'authentification 1983
Contrôle d'accès ServiceNow® 1994
Contrôle d’accès Exploree ServiceNow® 1995
Activer ServiceNow® le contrôle d’accès 1998

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer ServiceNow® le contrôle d’accès....2000
Journalisation d’audit....2001
Identité....2002
Analyseur d'accès....2003
Exploration de l’analyseur d’accès....2004
Utilisation de l’analyseur d’accès....2005
Évaluation de l’autorisation....2025
Forum aux questions....2027
Simulateur d'accès....2032
Aperçus d'accès....2046
Identité globale....2051
Explorer l’ID fédéré....2052
Accès aux critères d’ID fédéré....2053
Mise à jour des champs d’ID....2054
Audit d'identité et d'accès....2056
Exploration de l’audit d’identité et d’accès....2057
Résultats d’audit d’identité....2059
Champs auditables de sécurité....2062
Champs pris en charge et non pris en charge....2066
Identity Center....2067
Explorer Identity Center....2069
Activation d’Identity Center....2069
Identity Center pour les utilisateurs....2069
Mesures d’identité pour les administrateurs....2073
Console des identités des machines....2073
Exploration de la console d’identité de la machine....2074
Activation de la console d’identité de machine....2082
Utilisation de la console d’identité de la machine....2083
Système de gestion des identités interdomaines (SCIM)....2083
Fournisseur SCIM....2084
Client SCIM....2104
Observateur d’accès....2123
Configurer l’observation relative à l’accès....2123
Examiner les journaux de l’Observateur d’accès....2124
Ressources supplémentaires....2126

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécuriser votre instance

La sécurité de la plateforme fournit des options pour sécuriser l'instance.

ServiceNow Vault



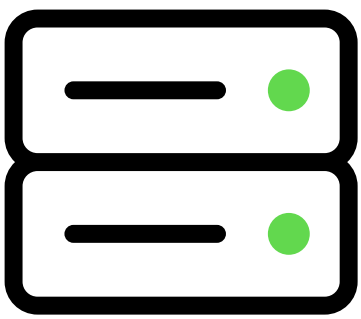
Utilisez l'ensemble d'outils de sécurité des données ServiceNow Vault qui protègent les informations sensibles contre tout accès non autorisé, la corruption ou le vol tout au long de leur cycle de vie.

Sécurité de la plateforme



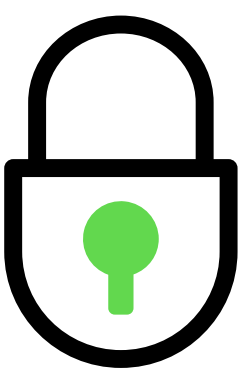
La sécurité de la plateforme fournit des options pour sécuriser l'instance.

Confidentialité de la plateforme



Confidentialité de la plateforme vous permet de masquer la date sensible sur l'instance.

Chiffrement



Protégez vos données sensibles et restez conforme aux exigences et normes réglementaires.

Gestion des accès



La gestion des accès vous permet d'accéder à l'instance ServiceNow en toute sécurité.

Identité



En savoir plus sur les identités dans l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Ressources supplémentaires pour les produits et solutions Platform Security



Explorez d’autres ressources de sécurité de la plateforme pour l’apprentissage.

Traduction automatique

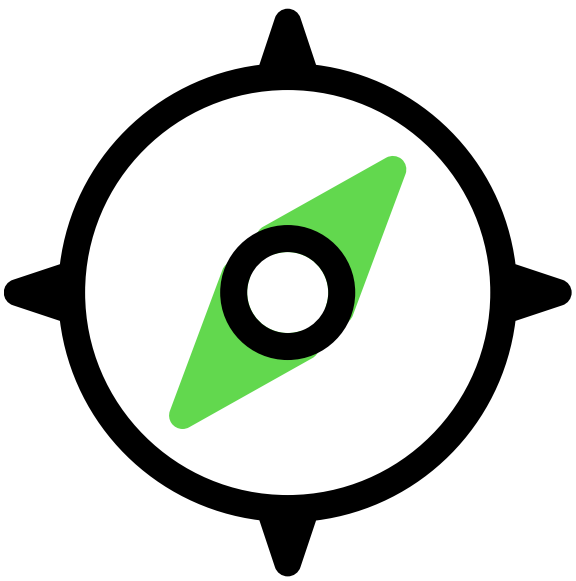
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Coffre-fort

ServiceNow Coffre-fort fournit un emplacement unique pour examiner et implémenter des outils de sécurité pour les exigences avancées en matière de sécurité et de confidentialité.

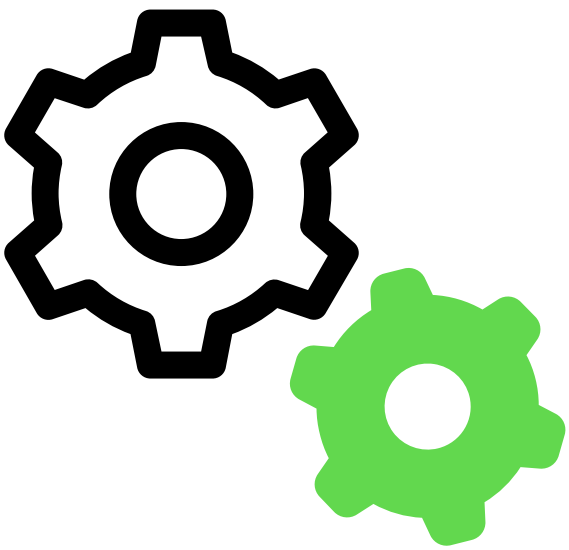
Premiers pas

Explorer ServiceNow Coffre-fort



En savoir plus sur ServiceNow Coffre-fort ses fonctionnalités

Configurer ServiceNow Coffre-fort

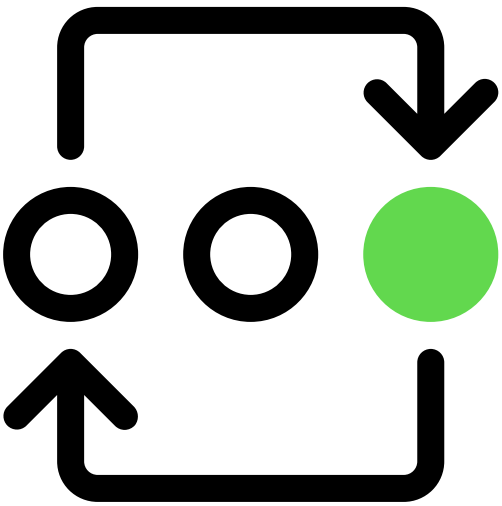


Introduction à l’installation et à la configuration ServiceNow Coffre-fort

Traduction automatique

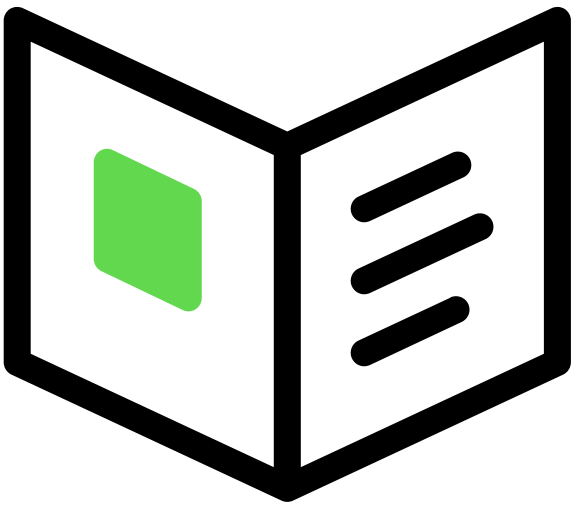
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de ServiceNow Coffre-fort



Découvrez comment utiliser le tableau de bord pour examiner la ServiceNow Coffre-fort sécurité de vos données.

Outils ServiceNow Coffre-fort



En savoir plus sur les outils utilisés avec ServiceNow Coffre-fort

Explorer ServiceNow Coffre-fort

En savoir plus sur ServiceNow Vault et passer en revue les avantages qu'il peut offrir pour vos besoins en matière de protection des données.

Vue d'ensemble de ServiceNow Coffre-fort

ServiceNow Coffre-fort est un ensemble d'outils de sécurité des données qui protègent les informations sensibles contre tout accès non autorisé, la corruption ou le vol tout au long de leur cycle de vie. Vous pouvez utiliser ServiceNow Coffre-fort pour appliquer des protections telles que le chiffrement, la gestion des secrets et la confidentialité des données pour la rédaction et l'audit des informations sensibles.

Remarque :

ServiceNow Coffre-fort est un module d'extension payant que ServiceNow le personnel doit activer sur votre instance de production. ServiceNow Coffre-fort inclut les composants répertoriés ici.

Pour acheter un abonnement, contactez votre chargé de compte ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si après avoir acheté un module d'extension, celui-ci n'est pas automatiquement activé, vous pouvez l'activer manuellement via la liste **Toutes les applications** de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Coffre-fort avantages

ServiceNow Coffre-fort avantages

Avantage	Fonctionnalité	Utilisateurs
Obtenez une vue d’ensemble complète ServiceNow Coffre-fort et passez en revue les mesures liées à la découverte, à la classification et à la protection de vos données	ServiceNow Coffre-fort Tableau de bord de la console	Administrateurs de la plateforme
Configurations guidées pour commencer facilement à utiliser les outils ServiceNow Vault avec des applications	Coffre-fort guidé	Administrateurs de la plateforme

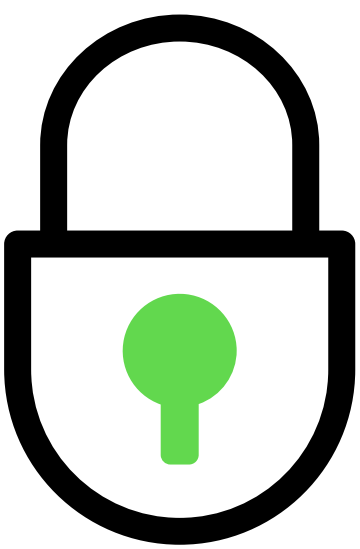
Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de ServiceNow Coffre-fort, consultez :

- ServiceNow Coffre-fort Tableau de bord de la console
- Configurer ServiceNow Coffre-fort
- Utiliser la configuration guidée pour ServiceNow Vault

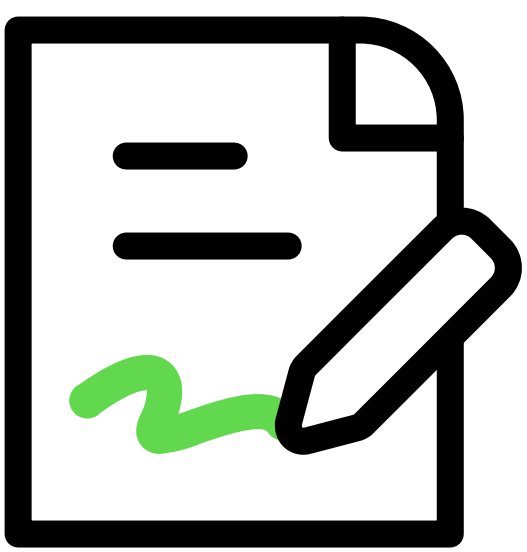
Outils ServiceNow Coffre-fort

Chiffrement



Gestion des clés et chiffrement des champs est une suite de modules de chiffrement hautement configurables

Signature de code



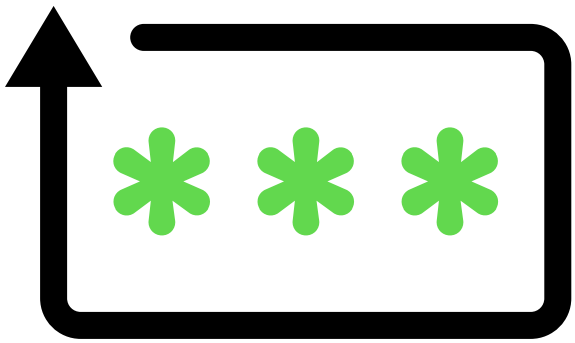
Améliorez la sécurité en validant les scripts et les données de configuration d'application sensibles avant leur utilisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Confidentialité des données



Utilisez le module d’extension Confidentialité des données pour supprimer les informations personnelles identifiables (PII) des données utilisateur lors de leur migration d’une instance de production vers une instance de non-production.

Découverte de données

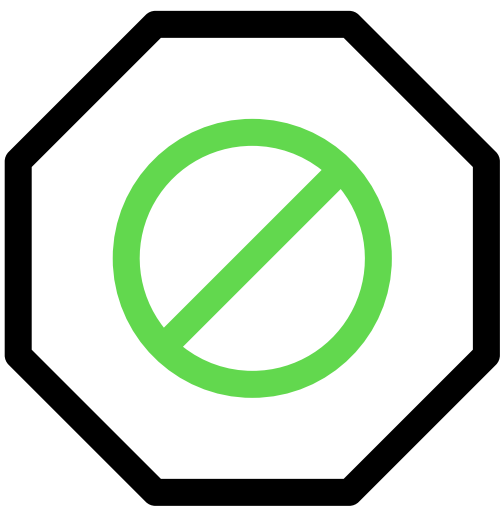


Le module d’extension Découverte de données vous permet de trouver des informations personnellement identifiables (PII) à partir des données utilisateur. Les données peuvent ensuite être classées pour d'autres mesures de sécurité.

Journaux



Accès zéro confiance



ServiceNow L’accès à la session permet aux organisations de réduire dynamiquement les privilèges de l’utilisateur dans une session Web

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Améliorez la sécurité, les performances et l'expérience utilisateur en important des données de journaux ServiceNow dans l'analyse des journaux d'entreprise à l'aide du service d'exportation de journaux.

Configurer ServiceNow Coffre-fort

Apprenez à installer et à configurer ServiceNow Coffre-fort

Vue d'ensemble de la configuration

- Installer les modules d’extension de l’archivage

  Découvrez comment installer ServiceNow Coffre-fort pour votre instance.

- Apprendre et configurer les rôles nécessaires à utiliser ServiceNow Coffre-fort

- Installer les modules d’extension de l’archivage

  Installez et vérifiez les plug-ins nécessaires pour tirer le meilleur parti de ServiceNow Coffre-fort.

Utilisation de la configuration guidée pour implémenter ServiceNow Coffre-fort

La configuration guidée fournit une séquence de tâches qui vous aident à configurer ServiceNow Coffre-fort votre instance ServiceNow. Pour ouvrir la configuration guidée pour ServiceNow Coffre-fort, accédez à **Tous** > **Coffre-fort** > **Console du coffre-fort**.

Pour plus d'informations, consultezCoffre-fort guidé.

Installer les modules d’extension de l’archivage

Découvrez comment examiner et installer les modules d’extension nécessaires pour ServiceNow Coffre-fort.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
ServiceNow Coffre-fort est une utilisation optimale avec d’autres produits de sécurité ServiceNow. Installez et configurez les autres modules d’extension pour tirer le meilleur parti de vos outils et mesures.

Procédure

1. Accédez à la **Tous** > **Coffre-fort** > **Console du coffre-fort**.
2. Passez en revue l’état de vos outils.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des outils

Statut	Description
Limited access	L'outil dispose d'une licence d'accès limité. Les mesures signalées peuvent être affectées ou indisponibles.
Included with platform	L'outil est inclus par défaut avec la plateforme
Needs license	L'outil n'a pas de licence. Les mesures signalées peuvent être affectées ou indisponibles.
Premium license	L'outil a un accès complet.

3. **Facultatif :** Si un état est limité ou a besoin d'une licence, passez en revue sa page d'installation respective.

Installation de l'outil

Outil	Page d'installation
Détection de données	Activer Détection de données
Classification des données	Inclus avec la plateforme
Anonymisation des données	Activer la confidentialité des données **Remarque :** L'anonymisation des données est installée dans le cadre de Confidentialité des données
Chiffrement de champ	Activer Chiffrement de champ
○ Accès zéro confiance (ZTA) ○ Authentification continue (CA)	○ Activation de l'accès zéro confiance ○ Activation de l'authentification continue

Utiliser la configuration guidée pour ServiceNow Vault

Utilisez la configuration guidée pour commencer à utiliser facilement une application avec ServiceNow Vault.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Coffre-fort** > **Console du coffre-fort**.
2. Dans la section **Coffre-fort guidé** , sélectionnez le bouton **Démarrer** pour votre application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans **Sélectionner les données de l'application**, utilisez la table pour sélectionner les données de l'application à utiliser avec , sélectionnez **Prévisualiser les classes** une ServiceNow Coffre-fort fois terminé

Sélectionner les champs de la table de données de l'application

Étiquette	Description
Table	Table dans laquelle se trouvent les données.
Colonne	La colonne dans laquelle se trouvent les données
Classe existante	Classification actuelle des données
Classe recommandée	Classification recommandée des données.
Application	Le périmètre de l'application des données

4. Dans **Prévisualiser la classification des données** , prévisualisez vos paramètres de classification des données, lorsque vous avez terminé, cochez Accepter et sélectionnez le bouton **Appliquer les classes recommandées** .

Prévisualiser les champs de table de classification des données

Étiquette	Description
Table	Table dans laquelle se trouvent les données.
Colonne	La colonne dans laquelle se trouvent les données
Classe finale	La classe à laquelle les données seront affectées
Application	Le périmètre de l'application des données

5. Dans **Résumé** de la classification, passez en revue les résultats de la classification des données, sélectionnez **Suivant** lorsque vous avez terminé.

Trouble?
Utilisez cette propriété Classification des données pour examiner toutes les données qui n'ont pas pu être classées.

6. Dans **Protéger les données existantes** , passez en revue les politiques de protection des données.

Protéger les champs de table de données existants

Étiquette	Description
Table	Table dans laquelle se trouvent les données.
Colonne	La colonne dans laquelle se trouvent les données
Anonymisation	Indique si une politique d'anonymisation des données peut être ou est déjà appliquée aux données.
Chiffrement de champ	Signale si une politique de chiffrement de champ peut être appliquée ou est déjà appliquée aux données.
Accès zéro confiance	Indique si une politique d'accès Zero Trust peut être ou est déjà appliquée aux données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. **Facultatif :** Vous pouvez sélectionner **Disponible** pour commencer à appliquer cette politique de protection des données d'application respective, consultez Mesures et mesures de coffre-fort pour plus d'informations.
8. Dans **Protéger les données en temps réel Passez** en revue vos politiques de protection des données en temps réel, sélectionnez **Marquer comme terminé** lorsque vous avez terminé.

Protéger les champs de données en temps réel

Étiquette	Description
Nom	Nom du ???
Type	Le type de canal de données.
Anonymisation en temps réel	Signale s'il existe une politique d'anonymisation en temps réel disponible ou déjà appliquée aux données.

Remarque :
Les données en temps réel seront protégées sur l'ensemble de l'instance et dans toutes les applications.

Résultats
L'application sélectionnée dispose désormais de données classifiées et de politiques de protection. De plus, il signalera désormais les mesures pertinentes au ServiceNow Coffre-fort Tableau de bord de la console.

ServiceNow Coffre-fort Tableau de bord de la console

Utilisez le tableau de bord de la ServiceNow Coffre-fort console pour suivre et gérer vos outils de sécurité ServiceNow Vault.

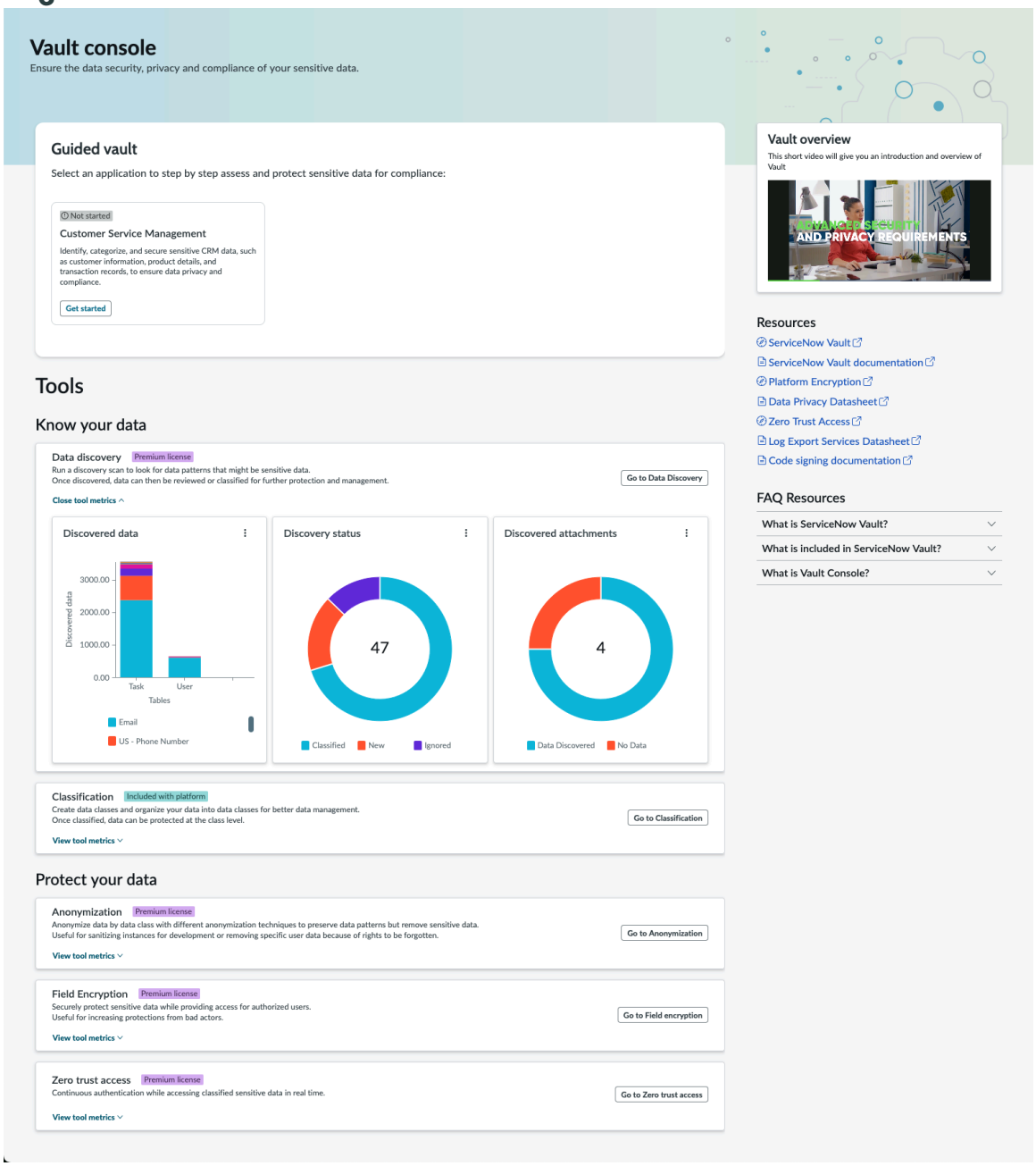
Le tableau de bord vous permet d'examiner facilement la sécurité, la confidentialité et la conformité de vos données sensibles. Le tableau de bord présente des rapports sur ServiceNow Coffre-fort les outils et leurs différentes mesures, et affiche des configurations guidées pour les applications compatibles avec ServiceNow Coffre-fort.

Pour accéder au tableau de bord de la ServiceNow Coffre-fort console, accédez à **Tous** > **Coffre-fort** > **Console du coffre-fort**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page du tableau de bord de la console du coffre-fort



Traduction automatique

Section	Sous-section	Description
Vue d’ensemble et ressources de la chambre forte	Vue d’ensemble de la chambre forte	Fournit une vue d’ensemble vidéo de ServiceNow Coffre-fort
	Ressources	Offre des ressources supplémentaires pour vous aider à utiliser ServiceNow Coffre-fort
	Ressources de la FAQ	Obtenez des réponses aux questions fréquemment posées sur ServiceNow Coffre-fort
Coffre-fort guidé	Cartes de configurations guidées pour les applications	Sélectionnez le bouton **Démarrer** sur une carte d’applications pour commencer à l’utiliser

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section	Sous-section	Description
		ServiceNow Coffre-fort avec cette application. Pour en savoir plus sur la configuration guidée, cliquez ici :Utiliser la configuration guidée pour ServiceNow Vault
Mesures et mesures de coffre-fort	Informations sur l'outil	Une brève description et des informations sur la gestion des licences pour les outils utilisés dans ServiceNow Coffre-fort. Sélectionnez le bouton **Accéder à** la page d'accueil des outils. Les outils actuellement affichés sur le tableau de bord sont les suivants : • Détection de données • Classification des données • Anonymisation des données • Chiffrement de champ • Accès zéro confiance (ZTA)
	Mesures de l'outil	Sélectionnez la liste déroulante pour passer en revue diverses mesures et graphiques sur un outil. **Remarque :** Pour plus d'informations sur les mesures, consultez la page d'accueil des outils respectifs,

Coffre-fort guidé

La configuration guidée du coffre-fort offre un processus étape par étape pour évaluer et protéger les données sensibles d'une application.

La configuration guidée du coffre-fort offre un moyen facile de commencer à utiliser ServiceNow Coffre-fort vos applications. Le programme d'installation utilisera les données des applications sélectionnées. La configuration aide d'abord l'utilisateur à examiner les données d'application pour la classification, puis aide à implémenter des politiques de protection sur les données classifiées. Vous pouvez consulter l'utilisation de la configuration guidée à l'adresse ServiceNow Coffre-fortUtiliser la configuration guidée pour ServiceNow Vault

Il y a 5 étapes dans une configuration guidée :

1. Sélectionner des données d'application
2. Aperçu de la classification des données
3. Résumé de la classification
4. Protéger les données existantes
5. Protéger les données en temps réel

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après une configuration guidée du coffre-fort, vous pouvez examiner les mesures des données de l'application dans la section **Outils** du tableau de bord de la console du coffre-fort. Pour en savoir plus, consultez la rubrique Mesures et mesures de coffre-fort.

Mesures et mesures de coffre-fort

Découvrez les outils et les mesures ServiceNow Coffre-fort utilisés pour protéger et détecter les données sensibles.

ServiceNow Coffre-fort s'intègre à plusieurs outils pour vous fournir une vue d'ensemble cohérente de la sécurité de vos données sensibles. Vous pouvez survoler un widget pour obtenir un aperçu plus approfondi des données signalées. Sélectionnez le bouton **Accéder à** sur n'importe quel outil pour accéder à sa page respective.

Connaissez vos données

ServiceNow Coffre-fort utilise Détection de données et Classification des données vous aide à comprendre et à connaître vos données.

Outils et mesures

Outil	Mesure	Description
Discovery Utilisez cette option Détection de données pour exécuter une analyse de découverte afin de rechercher des schémas de données susceptibles d'être des données sensibles. Une fois découvertes, les données peuvent ensuite être examinées ou classées pour une protection et une gestion plus approfondies.	Données découvertes	Histogramme détaillant les données détectées.
	Statut de découverte	Proportions d'états des données découvertes
	Pièces jointes détectées	Proportions de pièces jointes avec des données détectées.
Classification Classification des données Créer des classes de données et permet d'organiser vos données en classes de données pour une meilleure gestion. Les données classifiées peuvent être protégées au niveau de la classe.	Données classifiables	Proportions de données classifiables
	Données classifiées	Proportions de données classifiées

Protéger vos données

ServiceNow Coffre-fort utilise l'anonymisation des données, le chiffrement de champ et l'accès Zero Trust pour sécuriser et protéger vos données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Outils et mesures

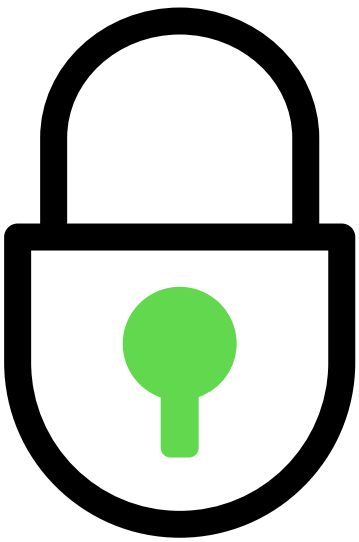
Anonymisation Anonymisez les données par classe de données avec différentes techniques d'anonymisation pour préserver les schémas de données, mais supprimez les données sensibles. Utile pour nettoyer les instances pour le développement ou pour supprimer des données utilisateur spécifiques en raison de droits à oublier. Les mesures sont les suivantes :	Graphique en temps réel ??	
	Données en temps réel	Histogramme montrant la quantité de données en temps réel anonymisées
	Temps d'exécution d'anonymisation	
Chiffrement de champ Protégez en toute sécurité les données sensibles tout en fournissant un accès aux utilisateurs autorisés. Utile pour renforcer les protections contre les mauvais acteurs.	État de classification des champs chiffrés	Proportion d'états de champs chiffrés
	Classes protégées par chiffrement de champ	Un tableau des classes protégées par le chiffrement de champ.
	Clés de chiffrement active	Affiche le nombre de clés de chiffrement actives. **Remarque :** Vous devez disposer du Key Management Framework rôle administrateur pour afficher ces données
Accès zéro confiance (ZTA) Authentification continue pendant l'accès aux données sensibles classifiées en temps réel.	État de classification de l'authentification continue	Proportion d'états de classification d'authentification continue
	Classes protégées par authentification continue	Affiche le nombre de classes protégées par authentification continue par leur classe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tous les ServiceNow Coffre-fort outils

Chiffrement



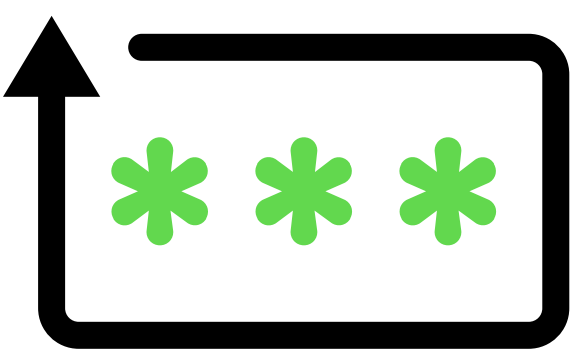
Gestion des clés et chiffrement des champs est une suite de modules de chiffrement hautement configurables

Signature de code



Améliorez la sécurité en validant les scripts et les données de configuration d'application sensibles avant leur utilisation.

Confidentialité des données



Découverte de données



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le module d’extension Confidentialité des données pour supprimer les informations personnelles identifiables (PII) des données utilisateur lors de leur migration d’une instance de production vers une instance de non-production.

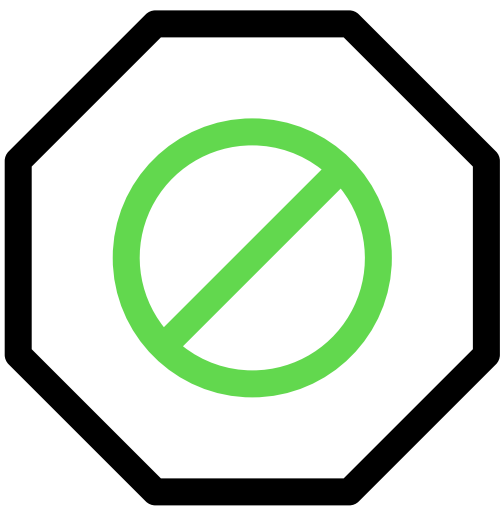
Le module d’extension Découverte de données vous permet de trouver des informations personnellement identifiables (PII) à partir des données utilisateur. Les données peuvent ensuite être classées pour d'autres mesures de sécurité.

Journaux



Améliorez la sécurité, les performances et l'expérience utilisateur en important des données de journaux ServiceNow dans l'analyse des journaux d'entreprise à l'aide du service d'exportation de journaux.

Accès zéro confiance



ServiceNow L’accès à la session permet aux organisations de réduire dynamiquement les privilèges de l’utilisateur dans une session Web

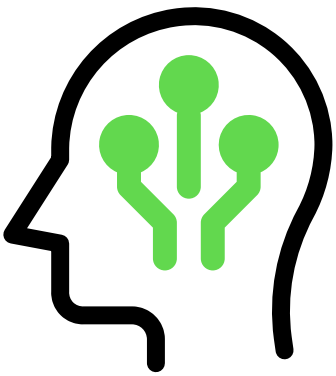
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurité de la plateforme

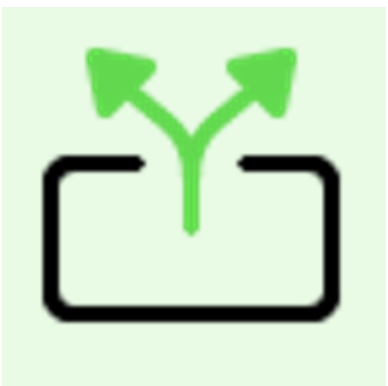
La sécurité de la plateforme fournit des options pour sécuriser l'instance.

Centre de sécurité



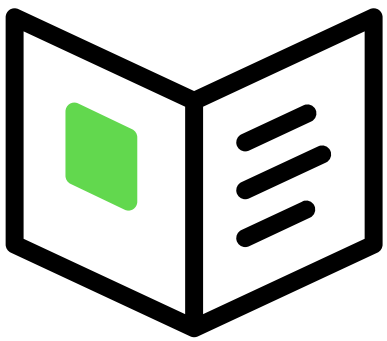
Permettez aux administrateurs de maintenir en permanence le plus haut niveau de posture de sécurité et surveillez facilement les événements et comportements non sécurisés.

Service d'exportation de journaux



Log Export Service (LES) vous permet d'exporter de manière transparente vos journaux d'instance, de système et d'application vers les outils d'analyse de sécurité de votre entreprise. Le service offre une intégration hautement évolutive et en temps quasi réel avec vos outils d'analyse, facile à configurer et à gérer.

Journaux



Le module Journaux fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Gestion des secrets



Signature de code



Options d'analyse antivirus



Traduction automatique

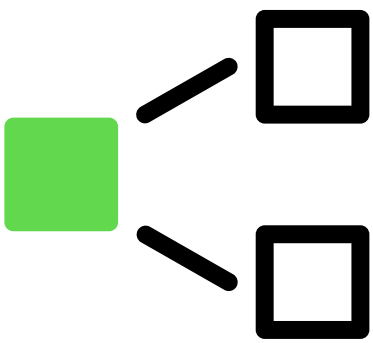
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l'accès à vos mots de passe en fonction des besoins de votre entreprise.

La signature de code crée des signatures numériques pour les données, qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données.

À utiliser Analyse antivirus pour protéger votre instance contre les infections virales qui peuvent être introduites par des pièces jointes dans vos enregistrements système, telles que les incidents, les problèmes et les stories.

Assainisseur HTML



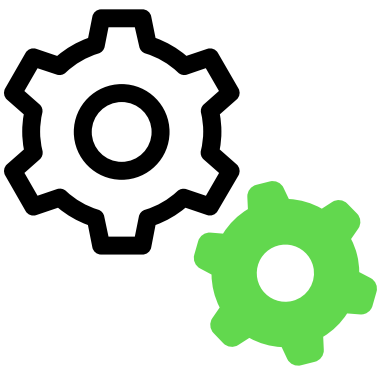
Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

Audit



Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

Paramètres de sécurité élevée



Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.

VPN (Virtual Private Network)



Paramètres de sécurisation renforcée



Traduction automatique

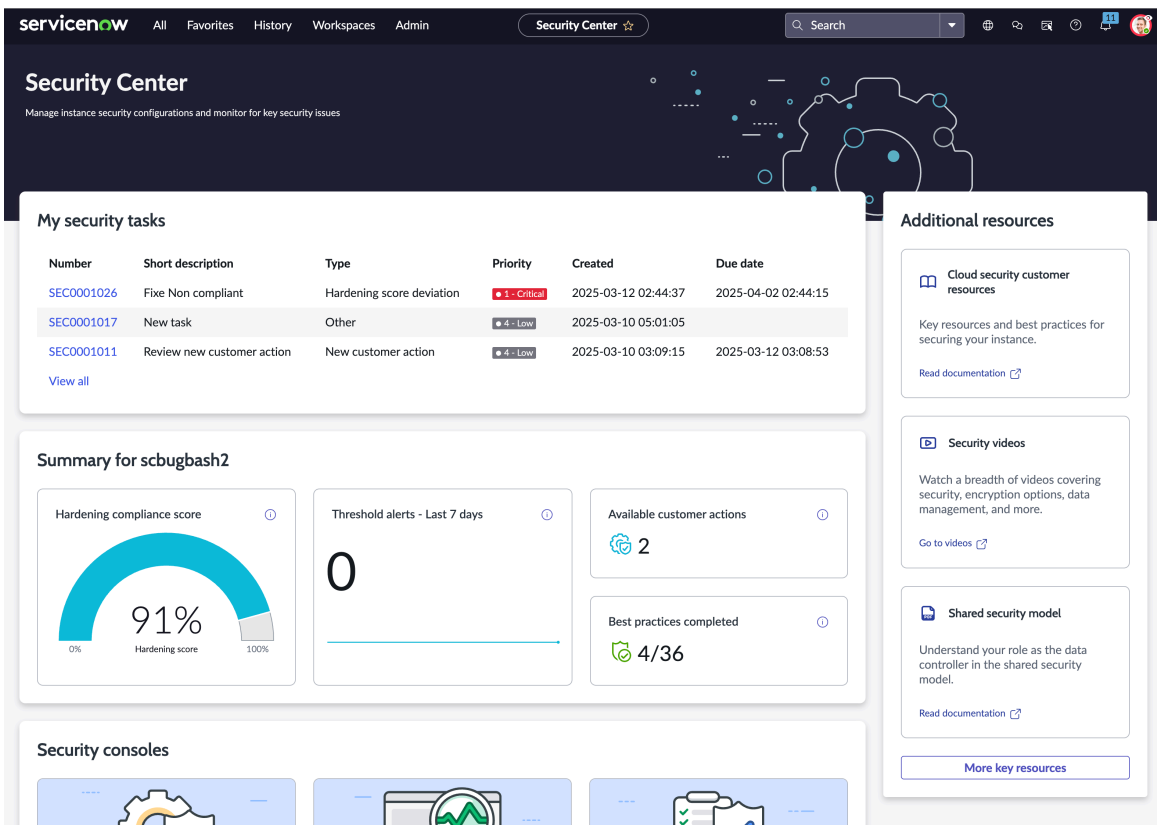
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.

Trouver des descriptions détaillées et des valeurs de conformité pour le contenu des paramètres de sécurisation renforcée du Centre de sécurité (SSC)

Centre de sécurité

ServiceNow Centre de sécurité est une application qui se compose d'un ensemble d'outils conçus pour aider votre organisation à maintenir la sécurité de vos déploiements ServiceNow. À l'aide de Security Center, vous pouvez améliorer la posture de sécurité et renforcer les niveaux de conformité avec une expérience utilisateur transparente.



Security Center est une application gratuite que les administrateurs peuvent télécharger à partir du ServiceNow Store. Il est installé par défaut à partir de la version Vancouver. Il est également disponible dans le ServiceNow Store tous les trimestres, entre les versions de famille, pour faciliter l'adoption plus rapide des nouvelles fonctionnalités.

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin de la commercialisation en septembre 2024 et n'est plus pris en charge ni disponible pour activation.

Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Premiers pas

Destination du centre de sécurité



Utilisez la page de destination du Centre de sécurité pour trouver les informations et les outils dont vous avez besoin pour sécuriser votre instance.

Console de configurations de sécurité



Utilisez la console de configuration de sécurité pour obtenir un aperçu rapide de la posture de sécurité de votre instance sur la page de vue d'ensemble.

Console de surveillance de Sécurité



Supervisez les notifications et les mesures de sécurité pour rester informé des risques de sécurité potentiels sur votre instance.

Console de posture de sécurité

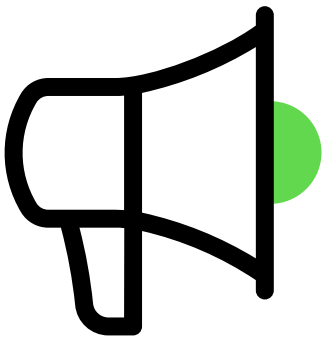


Améliorez votre posture de sécurité grâce à une visibilité complète et à des instructions détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Annonces de bannières de sécurité



Supervisez les notifications et les mesures de sécurité pour rester informé des risques de sécurité potentiels sur votre instance.

Dépannage et demande d'aide

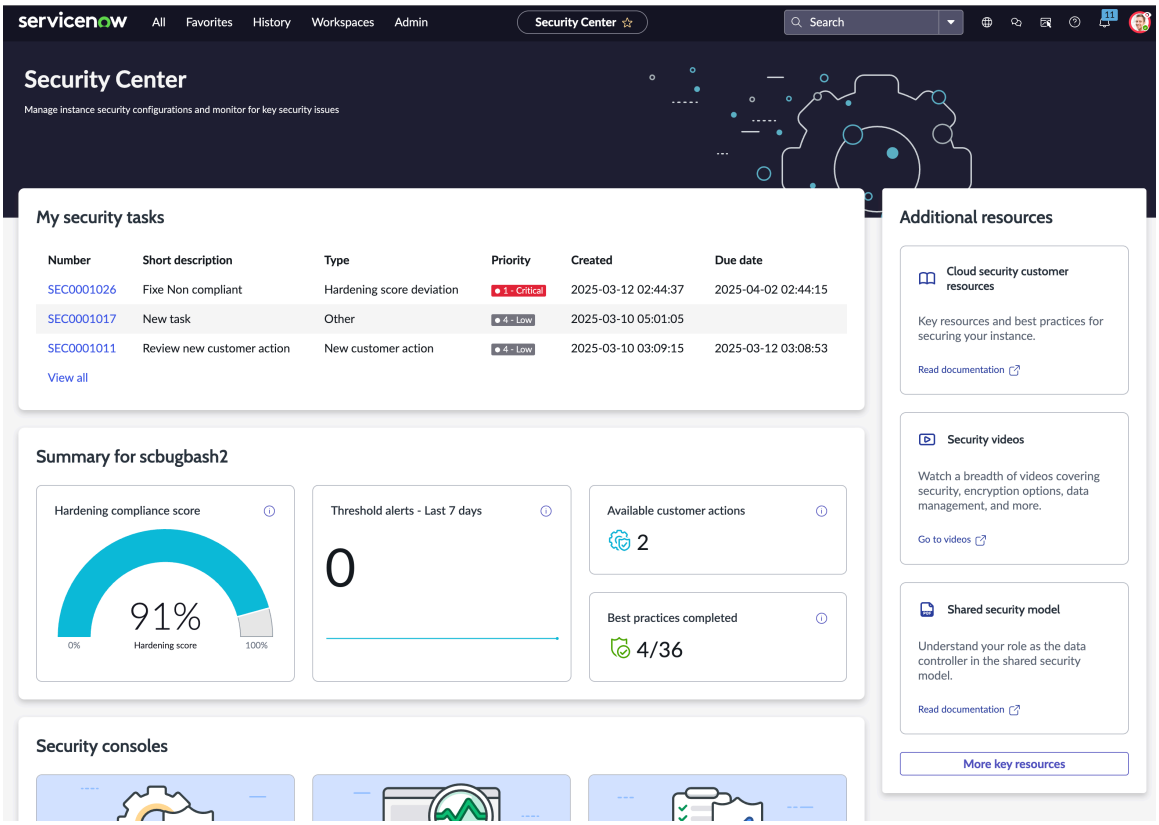
- Poser des questions et explorer d’autres ressources pour Centre de sécurité dans la section Opérations de sécurité de ServiceNow Community .
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Page de destination de Centre de sécurité

Utilisez la page de destination du Centre de sécurité pour trouver les informations et les outils dont vous avez besoin pour sécuriser votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Mes tâches de sécurité

La section Mes tâches de sécurité affiche une liste des tâches de sécurité qui vous sont affectées. Ouvrez une tâche en sélectionnant le numéro pour examiner les détails d'une tâche ou sélectionnez **Afficher tout** accéder au Gestionnaire des tâches de sécurité, où toutes les tâches sont visibles. Pour plus d'informations sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Résumé de l'instance

Le résumé de l'instance affiche une vue d'ensemble de haut niveau de l'état de la sécurité de votre instance. Sélectionnez l'icône d'informations (ⓘ) sur n'importe quelle carte pour obtenir des détails sur ce que chacune représente. Vous pouvez également sélectionner n'importe quelle carte pour naviguer vers la zone pertinente du centre de sécurité.

Gestion des identités et des accès

Utilisez les outils de la section Gestion des identités et des accès (IAM) Vérifiez que vos données ne sont accessibles qu'aux utilisateurs et aux processus qui en ont besoin. Pour plus d'informations sur ces outils, reportez-vous à la section Gestion des identités et des accès.

Consoles de sécurité

Sélectionnez une carte dans la section Consoles de sécurité pour accéder à l'une des trois consoles de sécurité.

- Console de configurations de sécurité
- Console de surveillance de Sécurité
- Console de posture de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

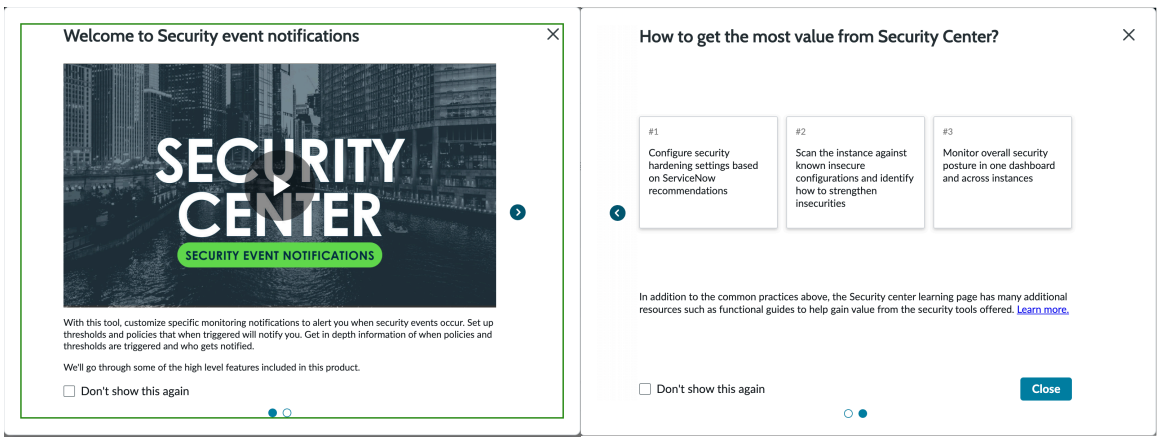
Outils

Utilisez la section Outils pour accéder aux outils dont vous avez besoin pour gérer la sécurité de votre instance. Ces outils sont organisés en trois onglets affichés en haut de la section. Sélectionnez une carte pour accéder à l'outil sélectionné.

Ressources supplémentaires

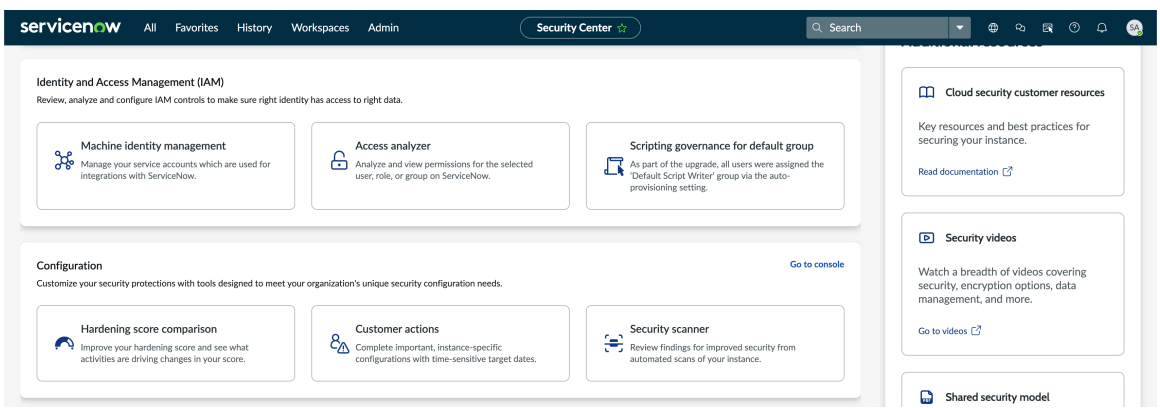
Utilisez la section Ressources supplémentaires située sur le bord de l'écran pour accéder à la documentation et aux vidéos relatives à l'apprentissage du Centre de sécurité, ainsi qu'à des informations sur la gestion de la sécurité de l'instance.

Le centre de sécurité a été mis à jour dans Zurich pour fournir des conseils afin de comprendre ce que l'outil peut faire et comment l'utiliser. Cette refonte est conçue pour aider les nouveaux utilisateurs et les utilisateurs occasionnels du centre de sécurité. De nouvelles fenêtres modales apparaissent dans le centre de sécurité pour montrer comment ces outils peuvent vous aider à atteindre vos objectifs de sécurité.



Gestion des identités et des accès

Utilisez les outils de la section Gestion des identités et des accès (IAM) Vérifiez que vos données ne sont accessibles qu'aux utilisateurs et aux processus qui en ont besoin.



IAM se compose de trois outils que vous pouvez utiliser pour gérer l'accès aux données sur votre instance.

Gestion de l'identité de la machine

Les identités de machine sont des informations d'identification numériques telles que des certificats, des clés et des jetons. Les serveurs, les applications, les conteneurs et les services cloud utilisent ces identités pour s'authentifier les uns avec les autres. Utilisez la **console**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'identité de machine pour gérer les identités de machine utilisées pour les intégrations avec ServiceNow.

Analyseur d'accès

Utilisez la console **Analyser l'accès et les autorisations** pour afficher les autorisations d'un utilisateur, d'un rôle ou d'un groupe sélectionné, ou pour comparer l'accès entre deux utilisateurs.

Scripting Governance pour le groupe par défaut

Utilisez l'outil de gouvernance des scripts pour configurer les préférences du groupe d'auteurs de scripts conditionnels. Les utilisateurs de ce groupe se voient attribuer le `snc_required_script_writer_permission` rôle, qui leur permet d'accéder aux scripts et aux champs de type script sur l'ensemble de la plateforme.

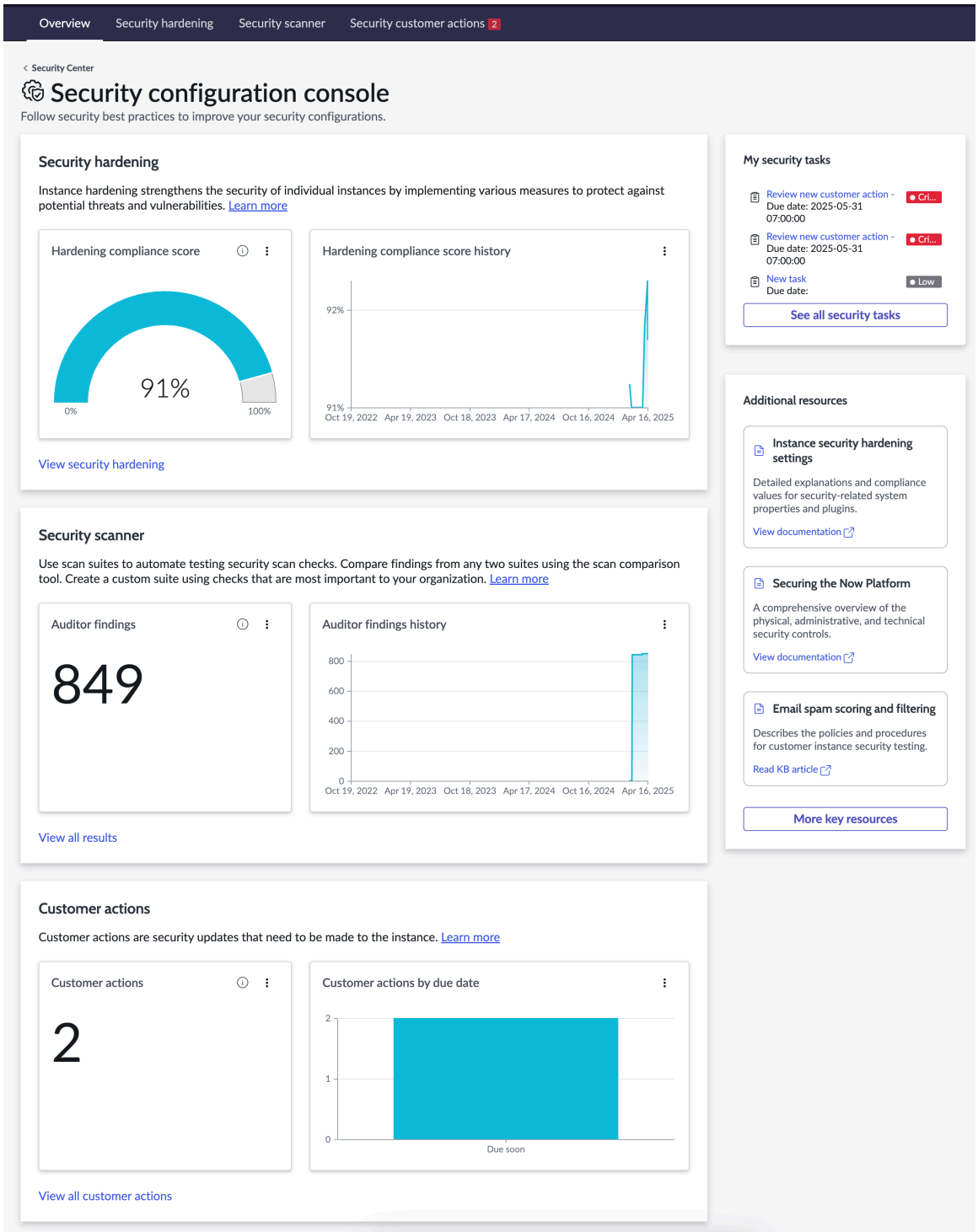
Avec les paramètres de cette console, vous pouvez activer ou désactiver l'affectation automatique de ce rôle, ainsi qu'affecter manuellement des utilisateurs au groupe. Vous pouvez également afficher des informations sur les personnes affectées et analyser votre instance pour trouver les utilisateurs qui ont scripté dans un délai spécifique.

Console de configurations de sécurité

Utilisez la page de configuration de la sécurité pour obtenir une vue d'ensemble de la posture de sécurité de votre instance. Consultez votre score de conformité à la sécurisation renforcée, découvrez les tendances graphiques, analysez les principaux paramètres de sécurisation renforcée non conformes et consultez les résultats de vos analyses de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Barre de navigation

Utilisez la barre en haut de la page pour naviguer entre cette page et la section Sécurisation renforcée de la sécurité, Scanner de sécurité ou Actions du client de sécurité du Centre de sécurité.

Sécurisation renforcée de la sécurité

Trouvez des détails sur votre conformité à la sécurisation renforcée dans la section Sécurisation renforcée de la sécurité. Sélectionnez les cartes dans cette section pour accéder à la Sécurisation renforcée de la sécurité page.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le score de conformité à la sécurisation renforcée est un pourcentage qui indique dans quelle mesure vos paramètres de sécurité s'alignent sur les paramètres recommandés. La section Sécurisation renforcée de la sécurité affiche ce pourcentage, ainsi que l'historique du score sur votre instance au fil du temps.

Scanner de sécurité

Examinez les résultats des contrôles de sécurité automatisés à l'aide de la section du scanner de sécurité. Ces vérifications vous aident à identifier les vulnérabilités de sécurité, les inefficacités et les problèmes de conformité.

Sélectionnez les cartes de cette section pour accéder à la page du scanner de sécurité.

Actions du client

Recherchez les mises à jour de sécurité qui peuvent être apportées à l'instance dans la section Actions du client. Cette section affiche le nombre d'actions disponibles et un graphique indiquant la date d'échéance de ces actions. Sélectionnez les cartes de cette section pour accéder à la page Actions du client.

Mes tâches de sécurité

Affichez les tâches de sécurité les plus urgentes qui vous sont affectées. Sélectionnez une tâche pour en afficher les détails, ou sélectionnez **Afficher toutes les tâches de sécurité** pour afficher une liste complète des tâches de sécurité.

Ressources supplémentaires

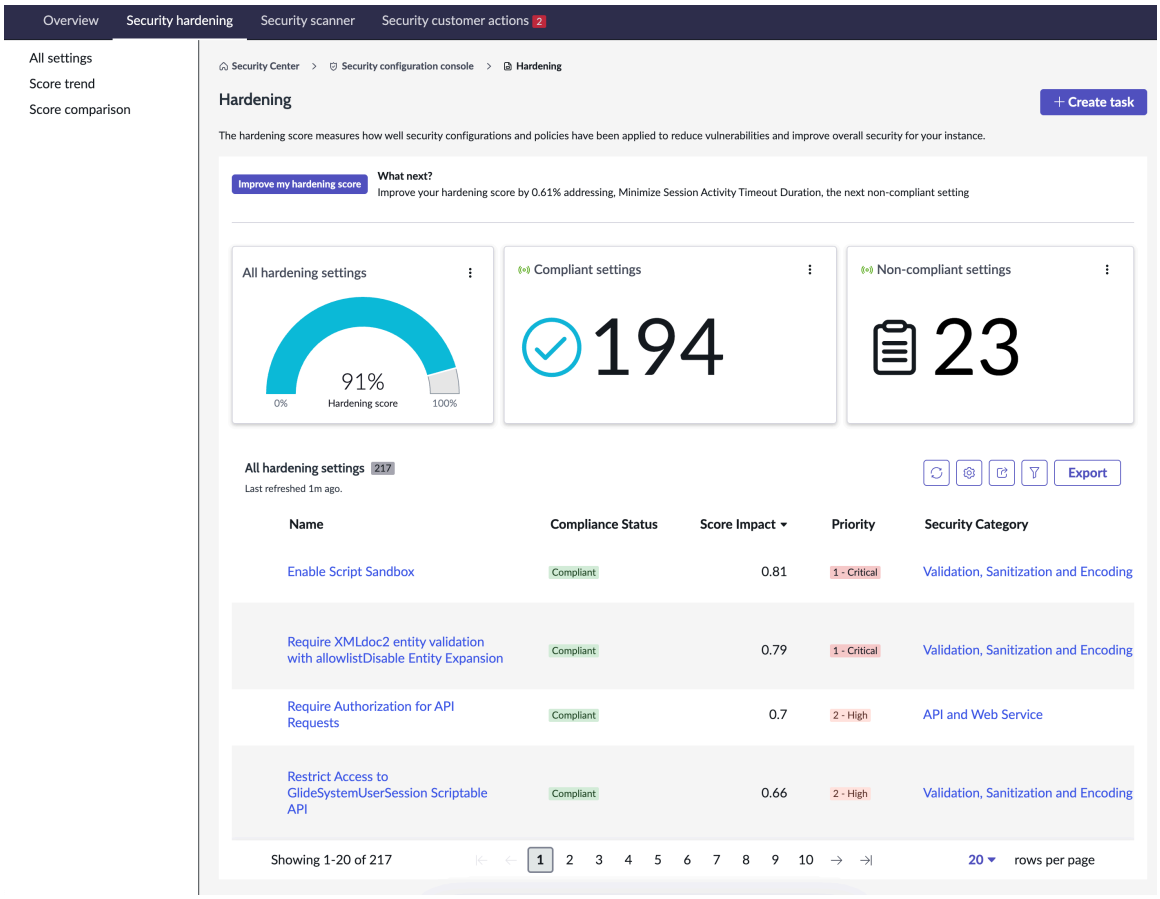
Utilisez la section Ressources supplémentaires située sur le bord de l'écran pour accéder à la documentation et aux vidéos relatives à l'apprentissage du Centre de sécurité, ainsi qu'à des informations sur la gestion de la sécurité de l'instance.

Sécurisation renforcée de la sécurité

Consultez votre score de conformité à la sécurisation renforcée, comparez-le aux scores précédents et modifiez les paramètres pour améliorer votre score de conformité et votre posture de sécurité sur la page de sécurisation renforcée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Paramètres de sécurisation renforcée Spécifiez des valeurs recommandées pour les propriétés et les modules d'extension liés à la sécurité dans le ServiceNow AI Platform. L'outil de sécurisation renforcée calcule le score de conformité du paramètre de sécurisation renforcée en pourcentage. Ce nombre indique dans quelle mesure votre instance est conforme aux paramètres de sécurisation renforcée du centre de sécurité.

Formule de calcul du score de conformité à la sécurisation renforcée :

- Chaque paramètre de sécurisation renforcée a un score de risque compris entre 0 et 10. Vous pouvez voir les valeurs des paramètres individuels dans la section **Tous les paramètres** .
- Le score est égal à la somme de tous les scores des risques de conformité divisée par la somme de tous les scores des risques.

Par exemple, la somme de tous les scores de risque de conformité est 25,4 et le total de tous les scores de risque est de 34,9. Pour cette somme, le score de conformité est de (25,4 /34,9) × 100, ce qui équivaut à 72,7. Cette décimale est arrondie au nombre entier le plus proche et sera donc égale à 73.

Ce calcul est effectué automatiquement le premier jour du mois, ou après une installation ou une réinstallation du Centre de ServiceNow sécurité. Vous pouvez déclencher un recalcul à tout moment à l'aide du bouton **Mettre à jour le score** sur cette page.

Sous-sections sur la sécurisation renforcée de la sécurité

La section Sécurisation renforcée de la sécurité contient trois sous-sections que vous pouvez sélectionner sur le bord gauche de l'écran.

Traduction automatique

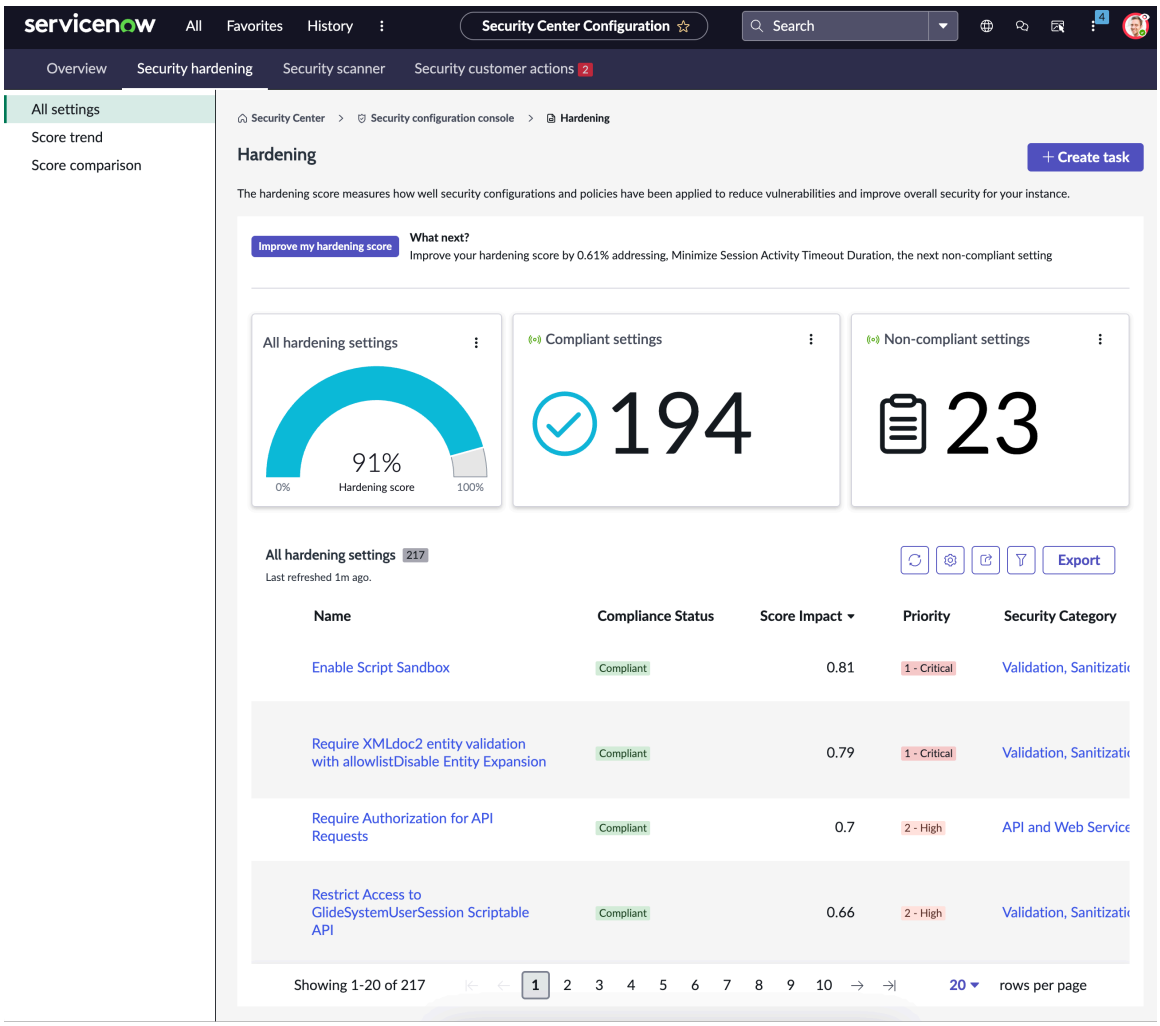
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Tous les paramètres
- Tendance du score de conformité à la sécurisation renforcée
- Comparaison des scores de sécurisation renforcée

Tous les paramètres

Passez en revue tous vos paramètres de sécurisation renforcée de l'instance disponibles sur une seule page.

La page **Tous les paramètres** affiche des informations sur tous les paramètres de sécurisation renforcée de l'instance. Utilisez les boutons en haut à droite pour actualiser, filtrer et exporter ces informations.\



Utilisez le bouton **+Créer une tâche** pour créer une tâche de sécurité afin d'effectuer une action du client. Ce bouton apparaît à la fois dans la page **Tous les paramètres** et dans les pages des paramètres de sécurisation renforcée individuels. Pour plus de détails, voir Tâches de sécurité.

Les informations suivantes sur les paramètres de sécurisation renforcée se trouvent dans la liste.

Nom

Nom du paramètre de sécurisation renforcée.

Statut de la conformité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indique si le paramètre est correctement configuré en fonction des recommandations du système (conforme) ou doit être configuré (non conforme)

Impact du score

Impact de ce paramètre de sécurisation renforcée sur votre posture de sécurité, exprimé en pourcentage. La somme de tous les impacts du score est égale à 100 %.

Priorité

Criticité du paramètre : Critique, Élevée, Modérée et Faible. Un score plus élevé indique un impact et une priorité plus importants.

Catégorie de sécurité

Catégorie de sécurité de la propriété. Sélectionnez la catégorie pour afficher les détails.

Détails de la résolution

Description des étapes pour corriger la vulnérabilité de sécurité du paramètre de sécurisation renforcée.

Pour savoir comment configurer un paramètre de sécurisation renforcée des propriétés, reportez-vous à la section Augmenter le score de conformité à la sécurisation renforcée.

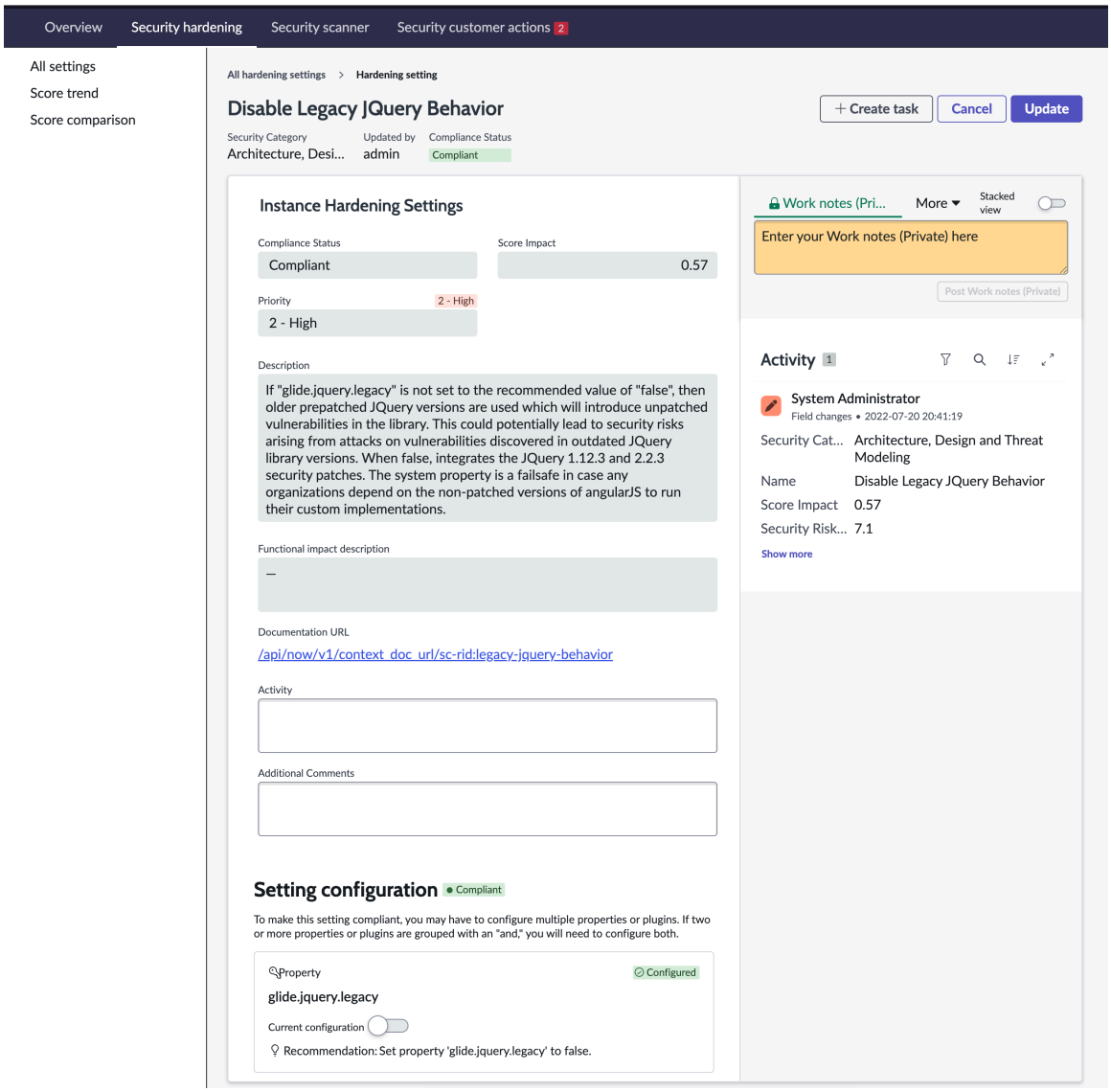
Détails des paramètres de sécurisation renforcée

Analysez les détails d'un paramètre de sécurisation renforcée en sélectionnant son lien dans l'application Centre de sécurité.

Accédez à la **Sécurisation renforcée** > **Tous les paramètres**, puis sélectionnez un paramètre de sécurisation renforcée pour être redirigé vers une page de l'outil de configuration de sécurisation renforcée qui affiche ses informations relatives à la sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Utilisez le bouton **+Créer une tâche** pour créer une tâche de sécurité afin d'effectuer une action du client. Pour plus de détails, voir Tâches de sécurité.

Détails de la configuration des paramètres de sécurisation renforcée

Attribut de configuration	Description
État de la conformité	Indique si le paramètre de sécurisation renforcée est conforme ou non.
Impact du score	Pourcentage qui indique l'impact de ce paramètre de sécurisation renforcée sur votre posture de sécurité.
Priorité	Un nombre compris entre 1 et 4, 1 ayant le poids le plus important qui indique l'intensité de l'impact que ce paramètre de sécurisation renforcée a sur votre posture de sécurité.
Impact fonctionnel	Impact de ce paramètre de sécurisation renforcée sur le fonctionnement de votre instance.
Description	Un aperçu général du paramètre de durcissement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de la configuration des paramètres de sécurisation renforcée (suite)

Attribut de configuration	Description
Documentation Url	Lien vers la documentation pour le paramètre de sécurisation renforcée.
Activité	Notifications des mises à jour liées au paramètre de sécurisation renforcée.
Configuration des paramètres	Détails relatifs à l'état de conformité de votre paramètre de sécurisation renforcée ainsi que des instructions sur la façon de les rendre conformes. **Remarque :** Certains paramètres de sécurisation renforcée peuvent nécessiter la configuration de plusieurs propriétés et modules d'extension pour les rendre conformes.

Paramètres de sécurisation renforcée des filtres

Simplifiez votre processus d'examen de la sécurisation renforcée à l'aide de filtres. Ces filtres peuvent créer une liste de travail des paramètres de sécurisation renforcée à examiner, qui sont restaurés pour une utilisation ultérieure et partagés avec d'autres utilisateurs.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité**.
2. Dans la section **Consoles de sécurité** , sélectionnez la **console de configuration de sécurité**.
3. Sélectionnez l'onglet **Sécurisation renforcée de la sécurité** .
4. Sélectionnez **Tous les paramètres**.
5. Sélectionnez le bouton **Afficher le panneau Filtre** ( ).
6. Dans la fenêtre **Filtre** , sélectionnez **Vue avancée**.
7. Créez un filtre affichant uniquement les paramètres de sécurisation renforcée que vous souhaitez examiner.
8. Une fois votre filtre terminé, sélectionnez **Enregistrer le filtre**.
9. Entrez un nom pour votre filtre et sélectionnez **Enregistrer**.

Remarque :
Vous pouvez également mettre cette liste à la disposition d'autres utilisateurs en définissant des autorisations sur **Tout le monde** ou **sur Groupe** pour la partager avec un groupe spécifique. Ces utilisateurs doivent également avoir l'autorisation d'utiliser le Centre de sécurité.

Que faire ensuite

Après avoir enregistré un filtre, vous pouvez le charger dans la **vue avancée** à l'aide du bouton **Utiliser le filtre existant** .

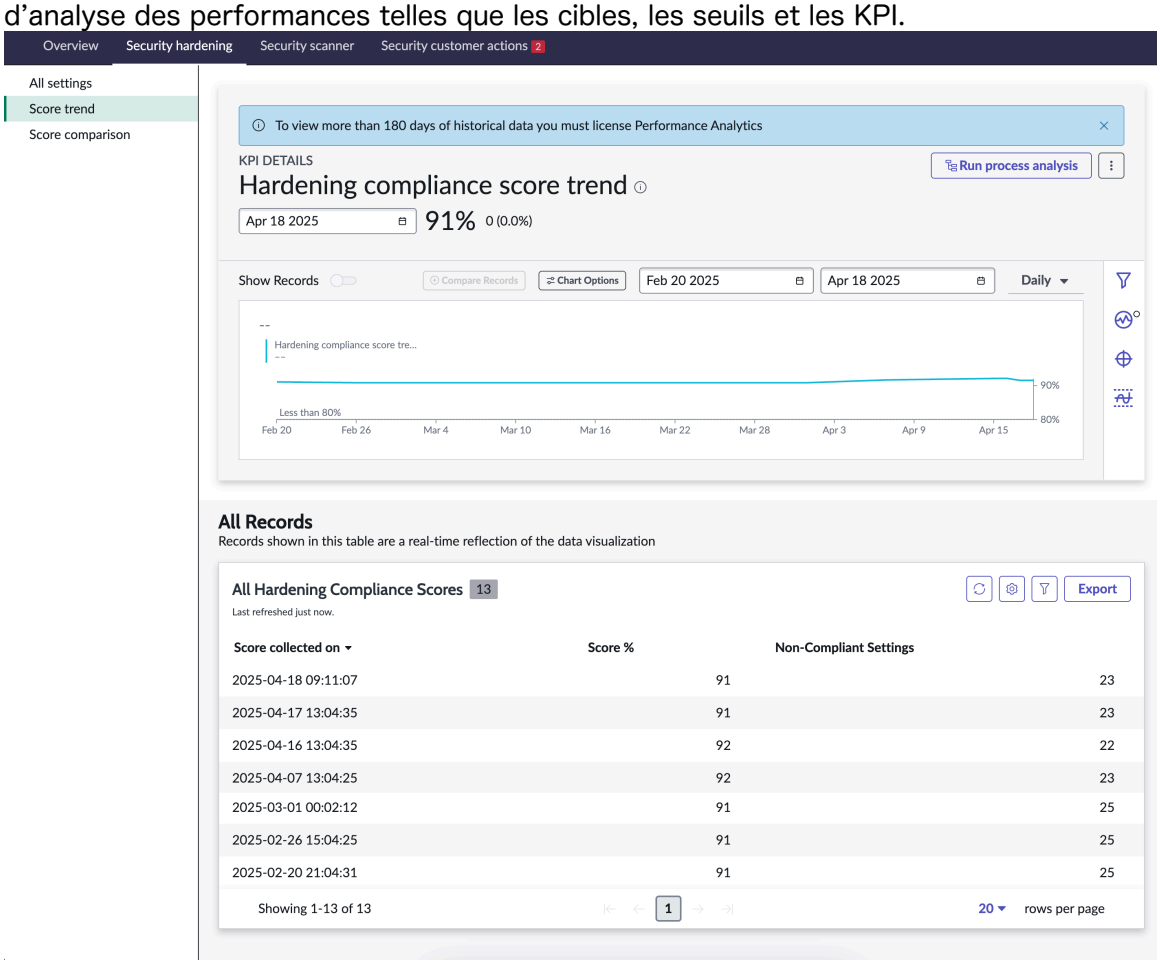
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tendance du score de conformité à la sécurisation renforcée

Affichez les tendances de votre score de conformité à la sécurisation renforcée au fil du temps dans un graphique ou un tableau.

Affichez les tendances de votre score de conformité dans le temps. Utilisez le sélecteur de dates pour sélectionner une période à analyser afin d'obtenir des informations sur les données en appliquant des fonctionnalités d'analyse des performances telles que les cibles, les seuils et les KPI.



Graphique des scores de conformité

Utilisez le bouton **Options du graphique** pour spécifier les informations à analyser et la façon de les présenter.

Analyse

Sélectionnez dans la liste des options. Certaines options peuvent ne pas être disponibles en fonction du type de graphique sélectionné.

Cible

Objectifs que votre organisation souhaite atteindre. Consultez Indicator targets .

Seuil

Définit une plage de scores normale pour un indicateur et vous alerte lorsqu'un certain événement se produit. Consultez Indicator thresholds .

Prévision

Décrit la possibilité de prévoir les scores futurs en fonction du comportement passé. Consultez Performance Analytics scores forecasts .

Graphique de tendance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Montre comment la valeur d’un ou de plusieurs éléments change au fil du temps.

Commentaires

Affiche des annotations sur des points de données individuels.

Étiquettes

Affiche les scores liés aux visualisations.

Statistiques

Affiche les statistiques relatives à votre score de conformité.

Séries chronologiques

Sélectionnez la mesure à afficher sur le graphique.

Score

Score de l’indicateur clé de performance (KPI).

Changement

Changement de score pour cet indicateur.

Changer le pourcentage

Changement en pourcentage des scores.

Type de diagramme

Sélectionnez un type de graphique pour contrôler la façon dont les informations que vous avez sélectionnées sont visualisées. Consultez Use cases for different time series visualization types .

Table Tous les enregistrements

La table Tous les enregistrements affiche la date à laquelle les scores de conformité ont été collectés, les pourcentages de scores et le nombre de paramètres non conformes. Vous pouvez utiliser cette table comme une autre option pour analyser la posture de sécurité de votre instance au fil du temps.

Augmenter le score de conformité à la sécurisation renforcée

Augmentez votre score de conformité à la sécurisation renforcée en vous assurant que les paramètres de sécurisation renforcée sont conformes aux recommandations du système.

Avant de commencer

Rôle requis : admin

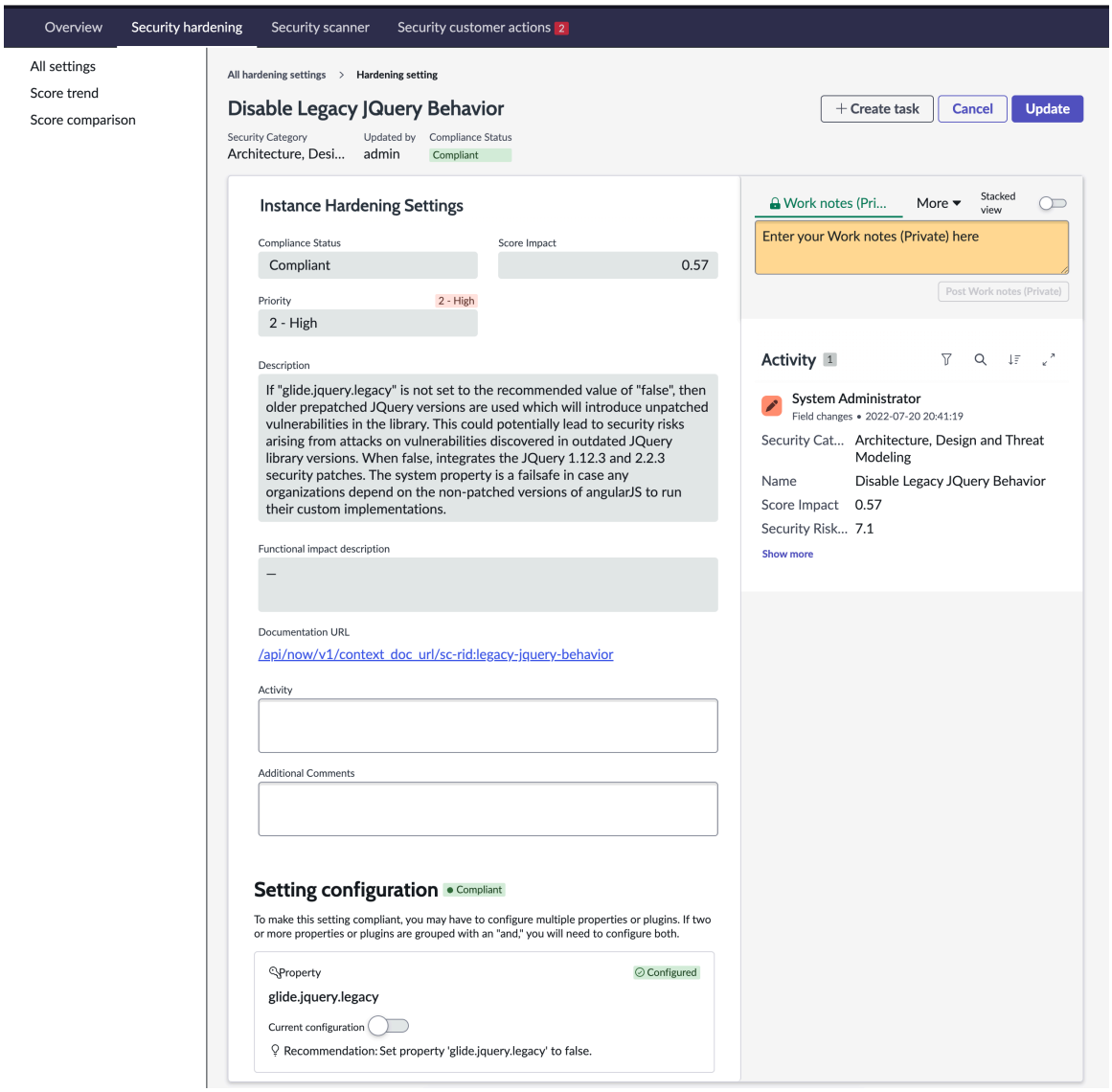
Identifiez les paramètres de sécurisation renforcée non conformes ayant l’impact de score le plus élevé sur votre instance. Examinez-les pour voir si vous pouvez vous conformer aux recommandations du système afin d’augmenter votre score de conformité global.

Procédure

1. Accédez à la **Sécurisation renforcée** > **Tous les paramètres**.
2. Filtrez la colonne Statut de conformité pour afficher uniquement les paramètres de sécurisation renforcée non conformes.
3. Sélectionnez **Impact du score** pour trier du plus grand au plus petit.
4. Sélectionnez des paramètres et examinez les détails des paramètres pour décider si vous souhaitez vous conformer aux recommandations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



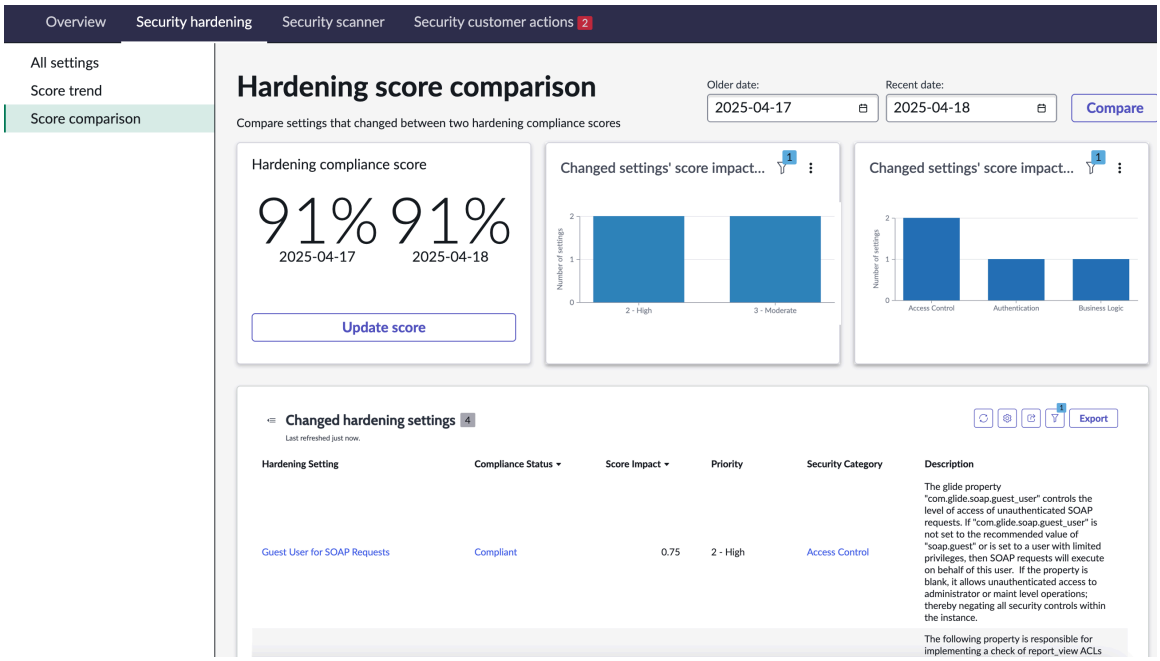
5. Rendez le réglage de durcissement conforme.
6. Si vous mettez à jour un score de sécurisation renforcée non conforme pour le rendre conforme, accédez à la page d'accueil et sélectionnez **Mettre à jour le score** pour afficher le score le plus à jour.
   Le score de durcissement est arrondi. Un score de 86,75 % sera arrondi à 87.

Comparaison des scores de sécurisation renforcée

Obtenez une visibilité sur l'intégrité de vos paramètres de sécurisation renforcée et utilisez ces données pour améliorer la posture de sécurité de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cette page affiche un résumé de votre conformité à la sécurisation renforcée et des changements apportés à votre instance qui ont un impact sur ce score.

La page de comparaison des scores de sécurisation renforcée affiche les paramètres de sécurisation renforcée avec les changements d'état de conformité entre les dates sélectionnées dans les champs **Date plus ancienne** et **Date récente** . Grâce à ces informations, vous pouvez voir comment ils ont influencé votre score de conformité à la sécurisation renforcée.

Score de conformité à la sécurisation renforcée

La carte compare le score de conformité de votre instance aux dates sélectionnées sous forme de pourcentage.

Impact du score des paramètres changés par priorité

Affiche le nombre de paramètres de sécurisation renforcée dont l'état de conformité a été modifié depuis la dernière mise à jour du score, organisés par valeur de priorité.

Impact du score des paramètres changés par domaine de sécurité

Affiche le nombre de paramètres de sécurisation renforcée qui ont changé l'état de conformité entre les deux dates sélectionnées, organisés par zone de sécurité.

Paramètres de sécurisation renforcée changés

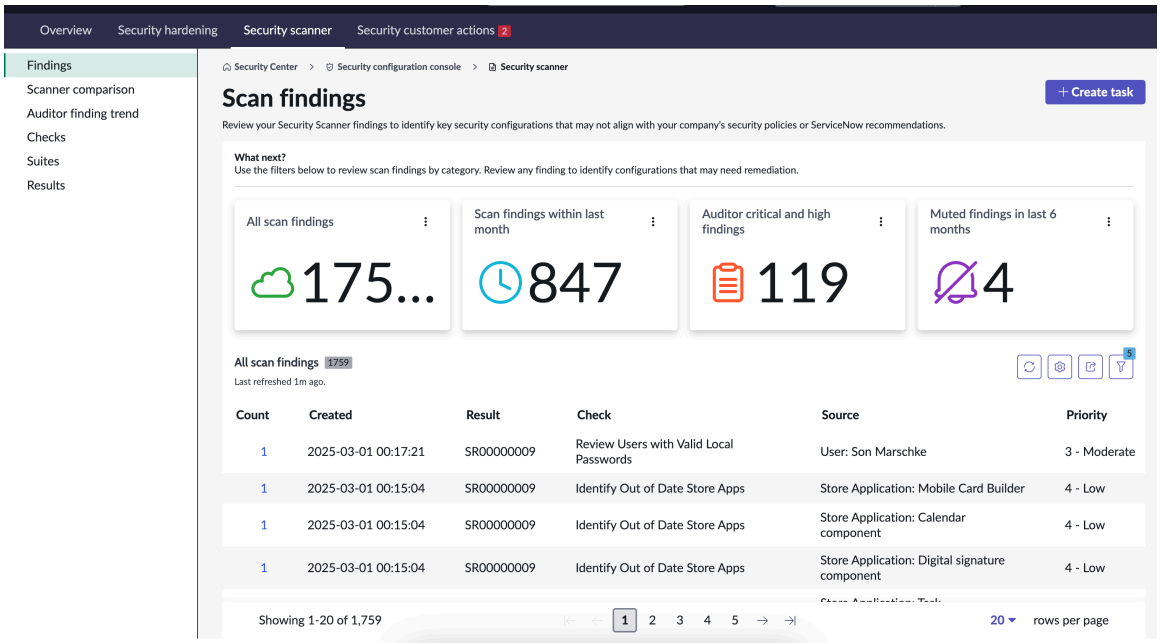
Affiche la liste des paramètres de sécurisation renforcée qui ont modifié les statuts de conformité entre les dates sélectionnées. Examinez les paramètres devenus non conformes et ayant diminué votre score de comparaison de sécurisation renforcée pour trouver des opportunités de les rendre conformes afin d'augmenter votre score. Consultez Augmenter le score de conformité à la sécurisation renforcée.

Scanner de sécurité

Analysez votre instance par rapport à un ensemble de contrôles de sécurité pour identifier une mauvaise configuration. L'outil de scanner simplifie le processus de création de différentes suites de vérifications pour différents cas d'utilisation afin que vous puissiez analyser les résultats au fil du temps.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

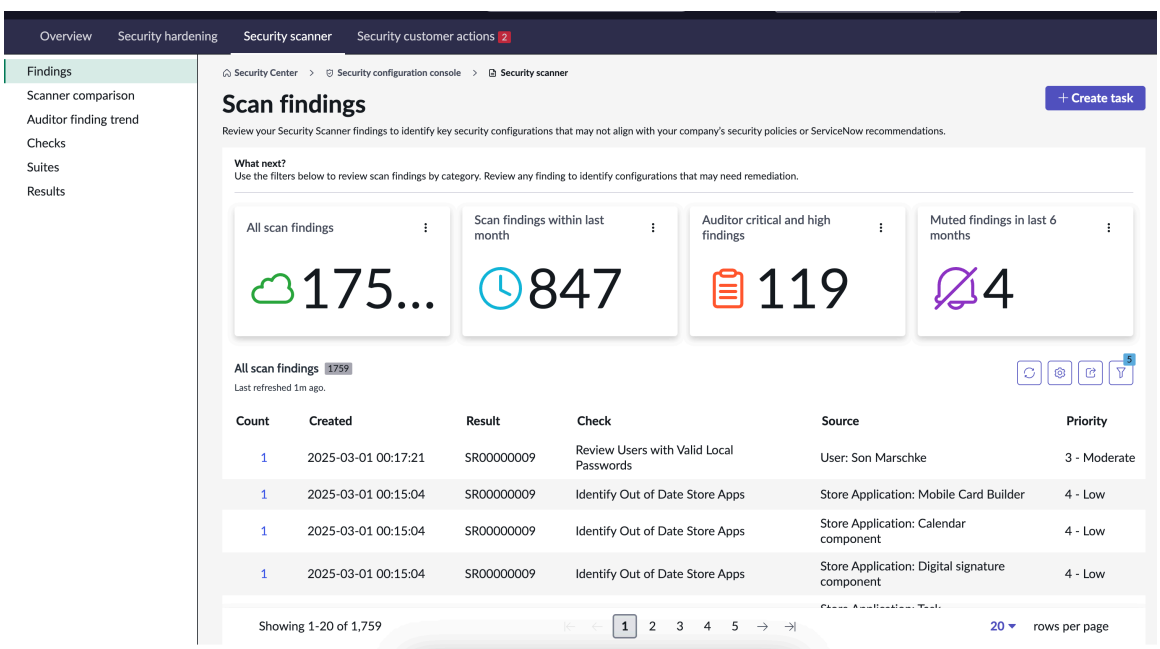


L'analyse de sécurité est une méthode permettant d'examiner votre instance à la recherche de configurations qui indiquent des problèmes d'intégrité de sécurité. Cette méthode vous permet d'identifier les opportunités d'implémentation de recommandations de sécurité pour votre organisation.

Lors de l'accès à l'outil de scanner, aucune comparaison n'est disponible tant que vous n'avez pas sélectionné la suite à comparer avec au moins deux résultats d'analyse de la suite. Vous pouvez utiliser la suite et les vérifications par défaut, ou vous pouvez créer vos propres vérifications et suites personnalisées.

Résultats d'analyse

Un résultat est une référence à un enregistrement qui a enfreint une règle à partir d'une vérification sur l'instance. Vous pouvez trouver l'enregistrement source et le nombre de fois où l'enregistrement a déclenché les règles d'une vérification donnée.



Traduction automatique

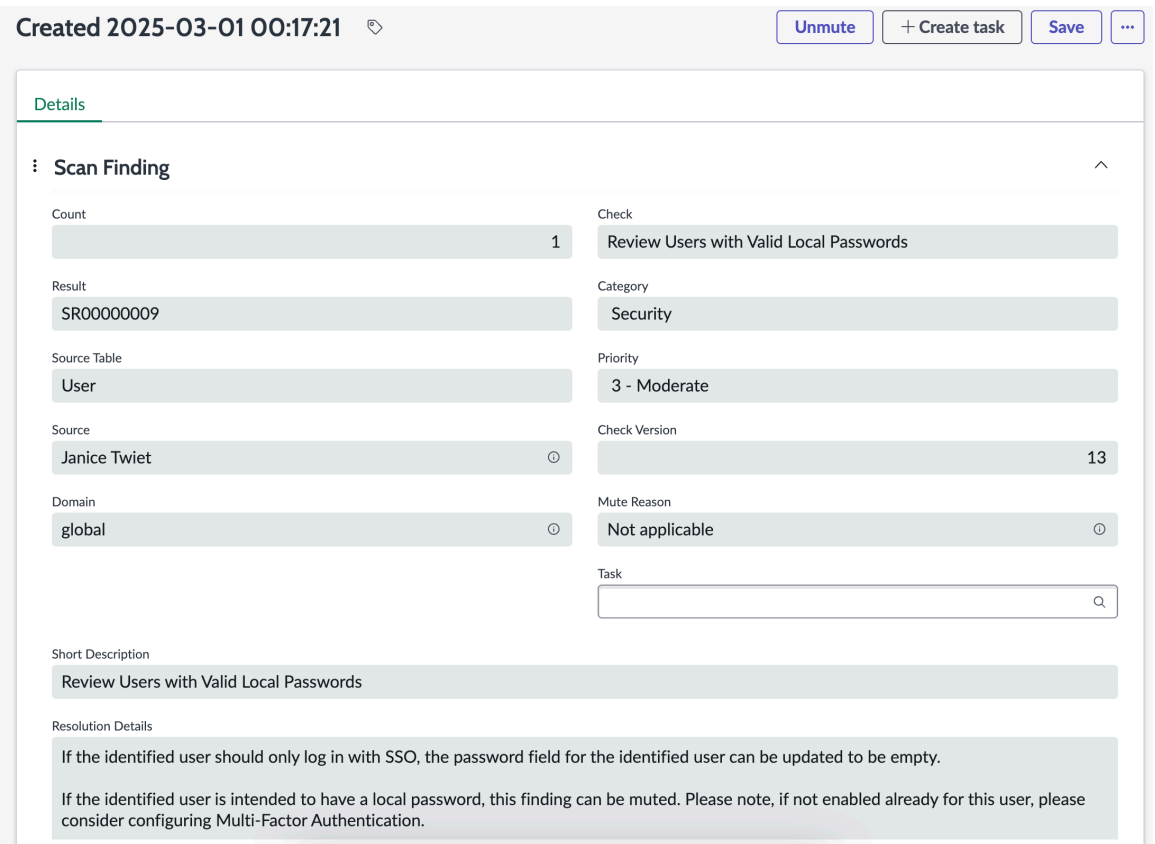
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accédez à l'onglet **Conclusions** pour afficher les conclusions de l'analyse dans une liste. Les cartes situées au-dessus de la liste indiquent le nombre de résultats qui correspondent à des critères spécifiques répertoriés sur la carte. Sélectionnez l'une de ces cartes pour filtrer la liste afin d'afficher uniquement celles qui correspondent aux critères.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité qui résout un résultat. Ce bouton apparaît à la fois sur la liste et dans l'enregistrement des résultats. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Résultats d'analyse

Sélectionnez un lien sous la colonne **Nombre** pour afficher un enregistrement des résultats, qui affiche les détails granulaires liés à un résultat spécifique.



Vérifier

Liste des vérifications associées à l'analyse.

Catégorie

Catégorie de sécurité associée à l'analyse. Par exemple, le contrôle d'accès ou le code malveillant.

Nombre

Nombre de fois où l'enregistrement a enfreint les règles de vérification.

Priorité

Gravité du risque de sécurité : 1 est la priorité la plus élevée tandis que 4 est la plus faible.

Résultat

Statut et type d'analyse.

Version de la vérification

Version de la vérification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table source

Enregistrement qui a enfreint une règle de la vérification.

Motif de désactivation

Raison de la mise en sourdine du résultat.

Source

Date à laquelle le résultat a été créé.

Tâche

Enregistrement de tâche associé à l'analyse. Utilisé pour faciliter les affectations de tâches à partir de la recherche d'un enregistrement.

Domaine

Domaine auquel l'analyse est appliquée.

Description brève

Brève explication de l'analyse.

Détails de la résolution

Instructions sur la façon de résoudre les problèmes signalés par l'analyse.

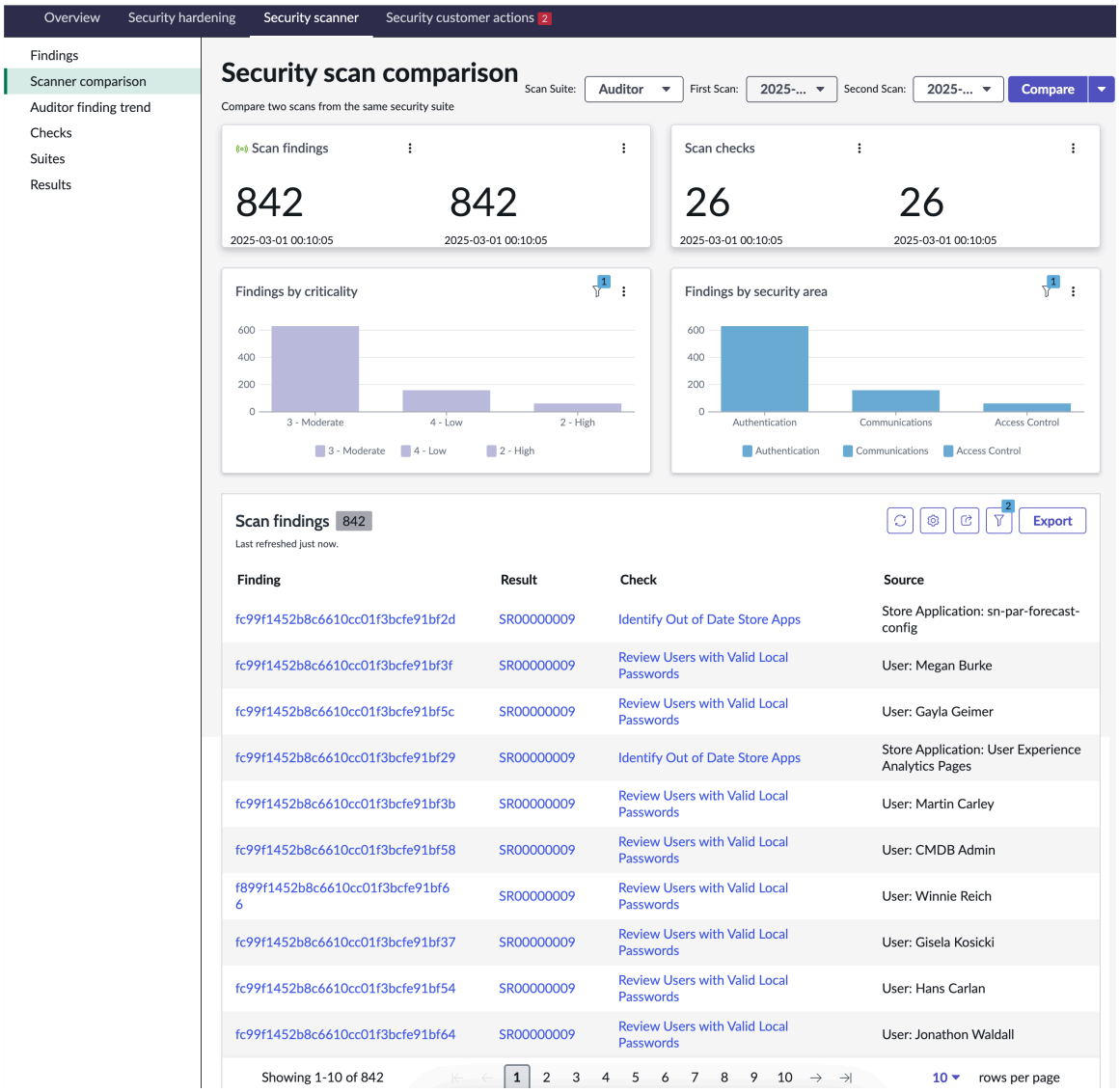
Les résultats peuvent être désactivés en sélectionnant le bouton **Activer/Désactiver le son** . Lorsque vous désactivez le son d'un résultat d'analyse, vous êtes invité à indiquer la raison de le désactiver. Les résultats atténués au cours des six derniers mois sont disponibles dans la carte des résultats atténués de la page **Conclusions de l'analyse** .

Comparaison de l'analyse de sécurité

Comparez deux analyses de la même suite de sécurité pour obtenir une visibilité sur l'intégrité de vos paramètres de sécurisation renforcée et améliorer la posture de sécurité de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Important :
Cette page est vide si vous n'avez pas deux instances ou plus de la même analyse à comparer. Exécutez une analyse au moins deux fois pour afficher une comparaison sur cette page.

Sélectionnez une analyse dans la liste **Suite d'analyse** , puis sélectionnez une **première analyse** et une **deuxième analyse** pour commencer une comparaison.

La page de comparaison des analyses de sécurité affiche les changements de sécurité dans vos paramètres de sécurisation renforcée entre la première et la deuxième analyse. Vous trouverez ci-dessous une explication de chaque carte :

Résultats d'analyse

Nombre de résultats de l'analyse sélectionnée à chaque date sélectionnée.

Vérifications d'analyse

Nombre de vérifications d'analyse effectuées dans l'analyse sélectionnée à chaque date sélectionnée.

Résultats changés par criticité

Graphique affichant tous les résultats classés par criticité.

Résultats changés par domaine de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

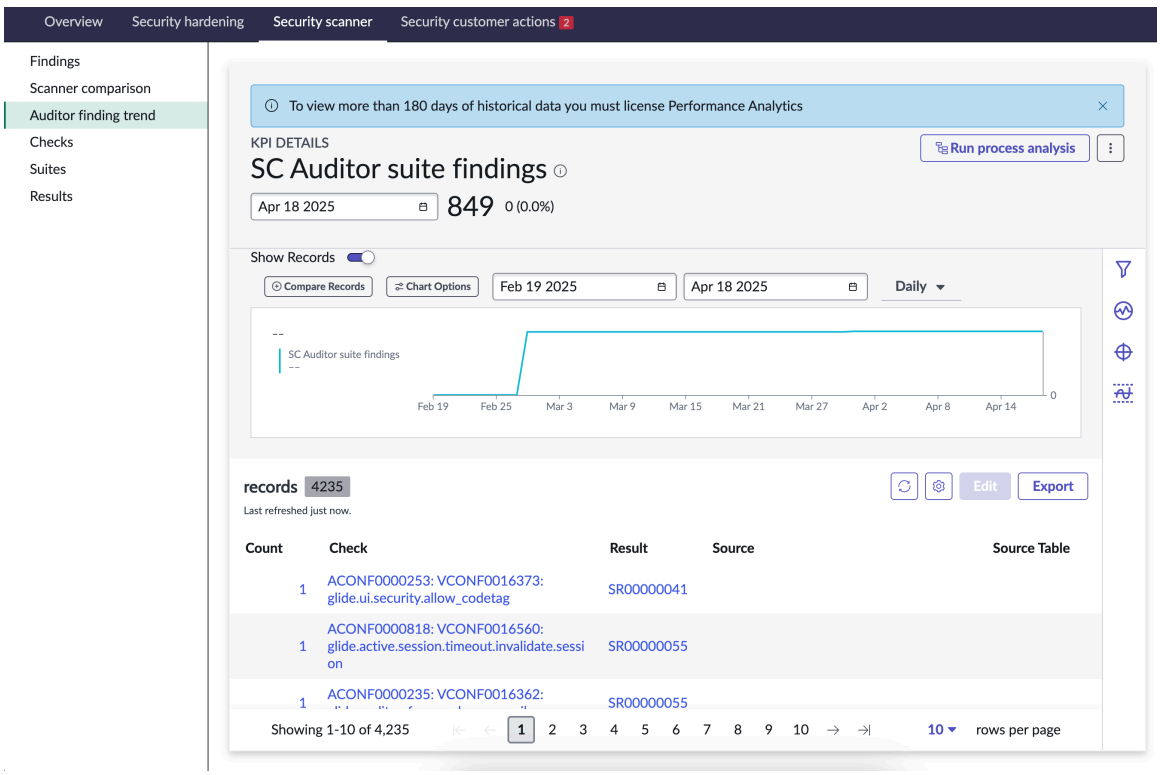
Graphique affichant tous les résultats zone de sécurité organisée.

Résultats d'analyse

Liste de toutes les conclusions de l'analyse. Sélectionnez une conclusion, un résultat d'analyse ou une coche pour afficher l'enregistrement associé et rechercher des détails supplémentaires. Utilisez les fenêtres inférieures en haut à droite pour filtrer, actualiser ou exporter la liste.

Résultats de la suite d'auditeurs

Passez en revue les résultats de la suite d'auditeurs du centre de sécurité au fil du temps.



Graphique des résultats de la suite d'auditeurs SC

La page affiche les résultats de la suite d'auditeurs SC comparés entre les deux dates sélectionnées. Utilisez le bouton **Options du graphique** pour spécifier les informations à analyser et la façon de les présenter.

Analyse

Sélectionnez dans la liste des options. Certaines options peuvent ne pas être disponibles en fonction du type de graphique sélectionné.

Cible

Objectifs que votre organisation souhaite atteindre. Consultez Indicator targets .

Seuil

Définit une plage de scores normale pour un indicateur et vous alerte lorsqu'un certain événement se produit. Consultez Indicator thresholds .

Prévision

Décrit la possibilité de prévoir les scores futurs en fonction du comportement passé. Consultez Performance Analytics scores forecasts .

Graphique de tendance

Montre comment la valeur d'un ou de plusieurs éléments change au fil du temps.

Commentaires

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affiche des annotations sur des points de données individuels.

Étiquettes

Affiche les scores liés aux visualisations.

Statistiques

Affiche les statistiques relatives à votre score de conformité.

Séries chronologiques

Sélectionnez la mesure à afficher sur le graphique.

Score

Score de l'indicateur clé de performance (KPI).

Changement

Changement de score pour cet indicateur.

Changer le pourcentage

Changement en pourcentage des scores.

Type de diagramme

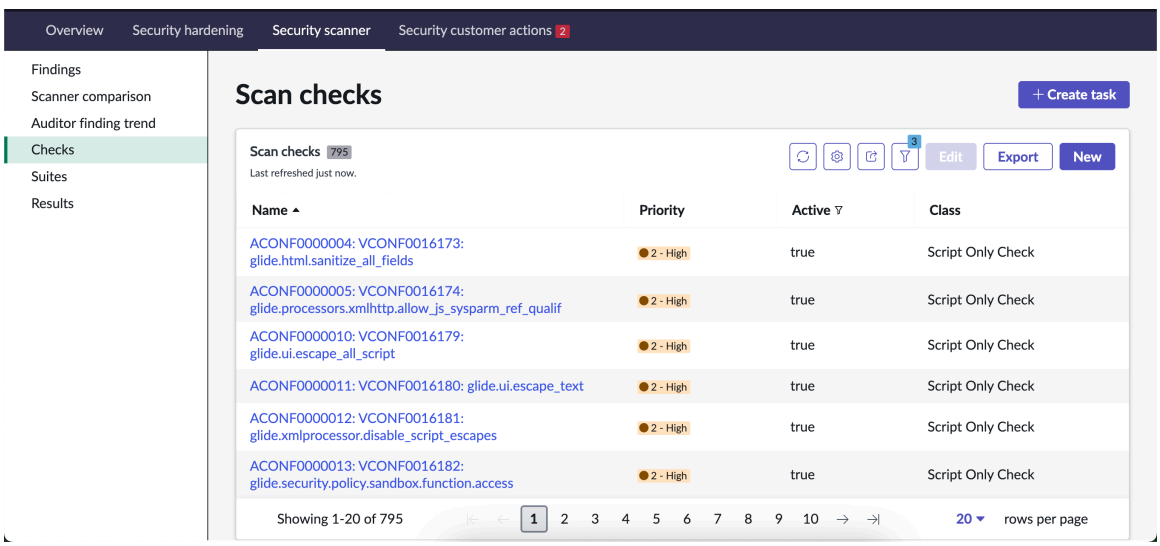
Sélectionnez un type de graphique pour contrôler la façon dont les informations que vous avez sélectionnées sont visualisées. Consultez Use cases for different time series visualization types .

Liste des enregistrements

Répertorie les vérifications effectuées dans le cadre de la suite.

Vérifications d'analyse

Utilisez les contrôles pour détecter les anomalies au sein d'une instance, en exécutant sur des tables, des enregistrements ou des métadonnées.



Les vérifications sont des règles conçues pour détecter les anomalies au sein d'une instance. Sélectionnez une vérification dans la liste pour afficher les détails, y compris ce que la vérification évalue et les étapes possibles pour corriger le problème si la vérification renvoie des conclusions.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité liée à une vérification d'analyse. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

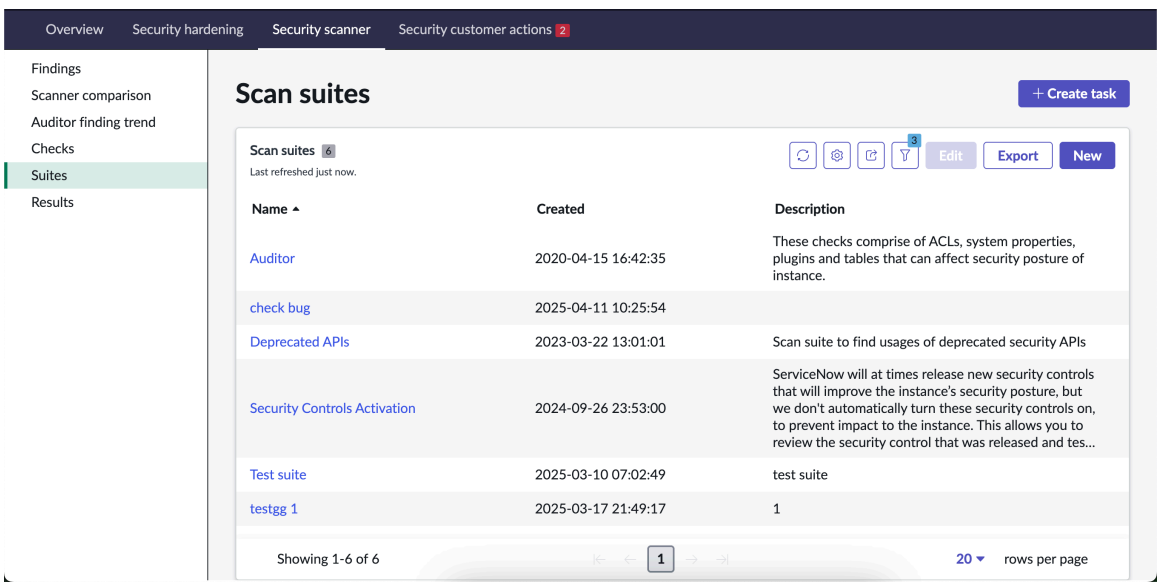
Les vérifications sont divisées en quatre classes pour identifier les problèmes et implémenter des recommandations de sécurité pour votre organisation : vérifications de table, vérifications de type de colonne, vérifications de script uniquement et vérifications de linter.

Vérifier les classes

Vérifier la classe	Description
Vérifications de table	Utilisez cette classe de vérification lorsque vous connaissez les tables et les vérifications spécifiques que vous voulez tester.
Vérifications de colonnes	Utilisez cette classe de vérification pour implémenter la règle que vous avez créée afin d'itérer tous les enregistrements correspondant au type de champ de colonne cible.
Vérifications de script	Utilisez cette classe de vérification pour vérifier les métadonnées et les configurations et exécuter des vérifications complexes en écrivant vos propres vérifications.
Vérifications Linter	Utilisez cette classe de vérification pour identifier tous les problèmes dans un script. Lorsqu'une vérification linter est exécutée sur un enregistrement, une arborescence syntaxique abstraite pour son code est générée, qui peut être utilisée pour analyser les problèmes avec le code.

Analyser les suites

Passez en revue les détails des suites d'analyse disponibles sur votre instance.



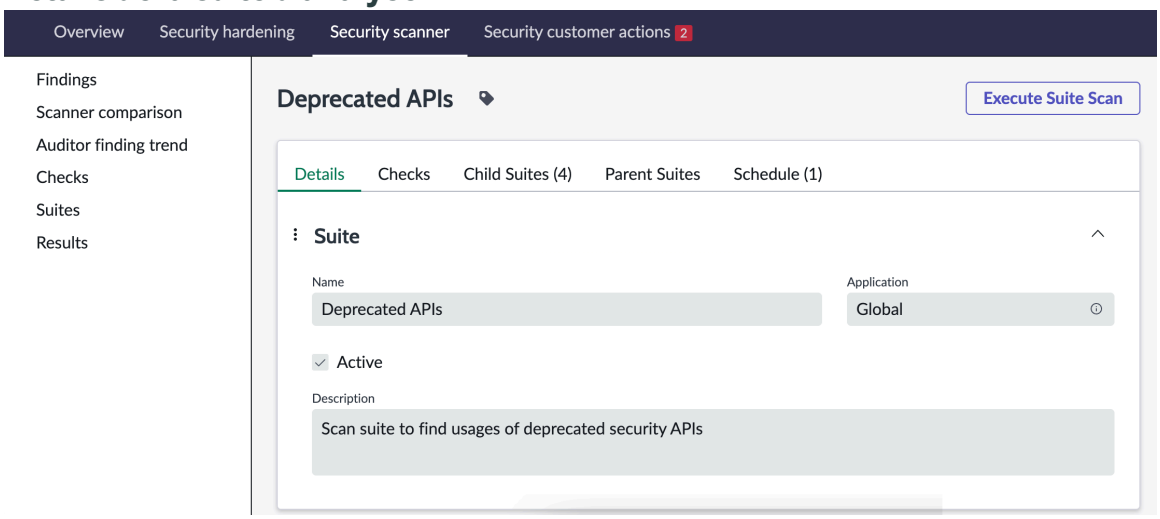
Les suites d'analyse sont des collections de vérifications du centre de sécurité qui s'exécutent ensemble. Vous pouvez utiliser des suites système de base ou créer les vôtres en clonant une suite existante et en mettant à jour les vérifications effectuées dans le clone. Pour plus de détails, voir Créer une suite d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une suite d'analyse. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Détails de la suite d'analyse



Sélectionnez le champ **Nom** d'une suite pour afficher les détails de celle-ci. Cette page fournit des détails sur les suites d'analyse dans une interface à onglets. Dans la page à onglets, vous trouverez les informations suivantes :

Détails

Les détails de la suite incluent son nom, son application et sa description.

Vérifications

Liste des vérifications incluses dans cette suite. Les détails sur les chèques individuels sont les mêmes que ceux que l'on trouve dans .Vérifications d'analyse

Suites enfants

Liste des suites enfants associées à cette suite. Lorsque vous exécutez cette suite, toutes les suites enfants s'exécutent également.

Suites parentes

Liste des suites dans lesquelles cette suite est une suite enfant. Lorsque vous exécutez une suite parente, cette suite est également exécutée.

Planifier

Détails de l'exécution planifiée de cette suite.

Contrôles des accès Vérifications de l'auditeur

Découvrez les vérifications disponibles dans les suites d'auditeurs de contrôles d'accès par défaut, les critères qu'elles évaluent et la façon dont elles peuvent être utilisées pour améliorer la sécurité de votre instance.

Les règles de liste de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Contrôles des accès Les vérifications d'auditeur évaluent votre instance en fonction des huit critères énumérés dans le tableau suivant. Utilisez les résultats de ces vérifications pour améliorer la sécurité de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur

Nom de vérification	Critères de vérification	Description
Tous les processeurs de type SCRIPT doivent être protégés avec un jeton CSRF	Recherche les processeurs avec le type **SCRIPT** qui ne sont pas protégés avec un jeton CSRF.	Tous les processeurs de type **SCRIPT** doivent être protégés avec un jeton de contrefaçon de requête de site à site (CSRF). L'option CSRF doit être cochée pour ces processeurs, ce qui interdit au processeur de s'exécuter à moins que l'instance n'utilise un jeton CSRF.
Peut contribuer/Impossible de contribuer aux critères d'utilisateur à définir sur chaque base de connaissances	Recherche les enregistrements de la base de connaissances pour lesquels les critères d'utilisateur **Peut contribuer** ou **Ne peut pas contribuer** sont définis.	Chaque base de connaissances doit avoir soit **le critère utilisateur Peut contribuer** , soit le critère utilisateur **Ne peut pas contribuer** défini. Dans le cas contraire, tout utilisateur peut contribuer au contenu d'une base de connaissances sans avoir de critères de contribution définis.
ACL vides	Recherche les enregistrements de liste de contrôle d'accès (ACL) qui n'ont aucun attribut de sécurité, aucun rôle ou le rôle **public** .	Si vous laissez les ACL vides ou utilisez le rôle **public** , vous pouvez ouvrir l'accès à tout contenu protégé par cette ACL.
Contrôles d'accès sur includes de script pouvant être appelé par le client	Recherche les includes de script appelables par le client qui ne sont pas sécurisés par des ACL.	Tous les includes de script pouvant être appelés par un client doivent être sécurisés avec une ACL à l'aide des rôles requis.
Accéder aux contrôles sur les pages de l'interface utilisateur	Recherche les pages de l'interface utilisateur qui ne sont pas sécurisées par des ACL	Sans ACL sécurisant l'accès à une page de l'interface utilisateur, cette page de l'interface utilisateur est accessible à tous les utilisateurs internes connectés. Sans aucune restriction, les utilisateurs connectés peuvent potentiellement effectuer des modifications non autorisées.
Accéder aux contrôles sur les tables	Recherche les tables sans ACL	Les tables doivent être sécurisées avec des ACL. L'accès aux données stockées dans les tables doit être limité aux seuls utilisateurs qui en ont besoin.
Le compte d'utilisateur ne doit pas avoir à la fois des rôles internes et externes	Recherche les enregistrements utilisateur avec des rôles **internes** et **externes** affectés	Les rôles d'utilisateur interne sont destinés aux utilisateurs de votre entreprise. Les rôles d'utilisateur externe sont destinés au personnel externe, comme les clients et les partenaires.
Base de connaissances et articles accessibles au public	Recherche les bases de connaissances et les articles de	Les bases de connaissances et les articles accessibles au public sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Critères de vérification	Description
	base de connaissances accessibles au public	visibles par tous les utilisateurs de l'instance. Augmentez la sécurité en limitant les bases de connaissances et les articles à l'audience spécifique qui en a besoin.

Vérifications de l'auditeur

Utilisez la suite Auditor pour SecureCheck afin de détecter les erreurs de configuration susceptibles d'impacter la posture de sécurité de votre instance.

Informations de vérification

Contrôles des accès Vérifications de l'auditeur

Nom de vérification	Description	Type de résultat de l'analyse
Identifier les applications de stockage obsolètes	Identifie les applications activées sur votre instance qui ont des versions mises à jour disponibles. Vérifiez que vous utilisez les versions les plus récentes des applications du magasin, qui peuvent inclure des correctifs pour les problèmes de sécurité potentiels.	Résolution recommandée
Appels GlideRecord non sécurisés	Identifie les scripts directement invocables par les utilisateurs finaux (tels que les includes de script pouvant être appelés par le client, les widgets, les processeurs, les points de terminaison REST) Ces scripts doivent respecter les ACL et utiliser GlideRecordSecure ou GlideRecord avec canRead, canWrite, canCreate, canDelete.	Résolution recommandée
Examiner les bibliothèques JavaScript autorisées	Identifie les scripts dans lesquels JavaScript Content Access Control est utilisé pour autoriser ou refuser des bibliothèques JavaScript tierces spécifiques. Examinez les personnalisations des instances pour vérifier que les bibliothèques ne sont pas utilisées avant de bloquer l'accès. La table Suivi de l'accès au fournisseur de contenu JavaScript [sys_js_content_provider_access_tracking]	Résolution recommandée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Description	Type de résultat de l'analyse
	peut être revue pour voir la date du dernier accès à la bibliothèque. **Remarque :** Cette vérification peut être ignorée dans les instances initialement mises en service à Tokyo ou une version ultérieure. Les enregistrements de la table associée ont des règles de refus définies par défaut. Dans les instances initialement mises en service avant Tokyo, il peut y avoir des règles d'autorisation dans les tables de contrôle d'accès JavaScript.	
Examiner les includes de script pouvant être appelés par le client sans ACL correspondante	Identifie les includes de script pouvant être appelés par les clients qui n'ont pas d'ACL correspondante. Ces scripts utilisent l'ACL d'include de script client pouvant être appelé par défaut (« * »). Pour ces scripts, créez des ACL qui définissent les critères d'accès appropriés pour vérifier que seuls les utilisateurs attendus peuvent interagir avec la fonctionnalité fournie.	Résolution recommandée
Passer en revue les tables personnalisées avec des créateurs d'enregistrements et aucune règle métier	Identifie les créateurs d'enregistrements qui n'ont pas de validation côté serveur supplémentaire. Cette vérification identifie les tables personnalisées avec un créateur d'enregistrement, mais sans règle métier associée. Ceux-ci peuvent permettre aux utilisateurs de soumettre des données inattendues dans la table associée.	Résolution recommandée
Examiner les ACL vides	Identifie les enregistrements ACL qui n'ont pas de script, de condition, d'attribut de sécurité ou de rôle, ou les ACL avec le rôle **public** . Laisser les ACL vides ou utiliser le rôle **public** permet d'accéder librement à tout contenu protégé par cette ACL.	Résolution recommandée
Examiner les champs avec HTML L'assainissement désactivé	Identifie les champs HTML dans lesquels l'assainissement HTML est inactif.	Résolution recommandée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Description	Type de résultat de l'analyse
	L'assainissement HTML supprime ou remplace les éléments et attributs potentiellement dangereux dans le code HTML. Examinez les champs HTML où le nettoyage est inactif pour confirmer si cette configuration est nécessaire.	
Examiner les modules d'extension de la fonctionnalité de sécurité inactifs	Identifie les modules d'extension non activés qui fournissent des contrôles de sécurité supplémentaires configurables. Les résultats de cette vérification sont fournis à titre informatif. Avant d'activer l'un des modules d'extension identifiés, vérifiez qu'il répond à vos cas d'utilisation ou à vos besoins. Vous pouvez désactiver le son de ces résultats si vous n'avez pas de cas d'utilisation pour l'élément identifié.	Informer
Examiner les plages d'adresses IP autorisées volumineuses	Identifie les plages de contrôle d'accès aux adresses IP qui contiennent un grand nombre d'adresses IP. **Remarque :** Si vous constatez un grand nombre de faux positifs, envisagez d'ajuster la variable largestExpectedCIDRBlock pour répondre à vos besoins professionnels spécifiques. Les blocs CIDR (Classless Inter-Domain Routing) contiennent une plus grande quantité d'adresses IP à mesure que le nombre diminue. Par exemple, la taille du bloc CIDR 8 est plus grande (contient plus d'adresses IP) que la taille du bloc CIDR 16. Vérifiez et confirmez que la configuration actuelle correspond aux besoins de votre entreprise.	Examiner et décider
Examiner les schémas GraphQL publics	Identifie les schémas GraphQL publics dans la table API GraphQL [sys_graphql_schema]. Ces schémas peuvent être configurés pour être disponibles sans authentification. Selon	Examiner et décider

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Description	Type de résultat de l'analyse
	la fonctionnalité du point de terminaison, cela peut permettre à des utilisateurs non authentifiés d'effectuer des actions inattendues ou d'interagir avec des données inattendues.	
Examiner les articles de la base de connaissances publique	Identifie les bases de connaissances et les articles de la base de connaissances configurés pour permettre l'accès aux utilisateurs non authentifiés. Vérifiez et confirmez que la configuration actuelle correspond aux besoins de votre entreprise.	Examiner et décider
Examiner les points de terminaison d'API REST publics	Identifie les points de terminaison d'API REST dans la table Ressource REST scriptée [sys_ws_operation] qui sont configurés pour être disponibles sans authentification. Selon la fonctionnalité du point de terminaison, cela peut permettre à des utilisateurs non authentifiés d'effectuer des actions inattendues ou d'interagir avec des données inattendues.	Examiner et décider
Examiner les pages du portail de services publics	Identifie les pages de Portail de services qui sont rendues publiques. Les pages du portail de services sont mises à la disposition des utilisateurs non authentifiés en définissant le champ « public » sur « vrai ». Vérifiez et confirmez que la configuration actuelle correspond aux besoins de votre entreprise.	Examiner et décider
Examiner les pages publiques de l'interface utilisateur	Identifie les pages de l'interface utilisateur qui sont rendues publiques. Les pages de l'interface utilisateur peuvent être mises à la disposition des utilisateurs non authentifiés à l'aide de la page [sys_public]. Vérifiez et confirmez que la configuration actuelle correspond aux besoins de votre entreprise.	Examiner et décider

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Description	Type de résultat de l'analyse
Examinez les rôles qui contiennent le rôle « administrateur »	Identifie tous les rôles (table Rôles [sys_user_role]) qui contiennent le rôle **administrateur** . Le rôle **administrateur** accorde aux utilisateurs des privilèges administratifs et ne doit être utilisé que lorsque cela est nécessaire. Vérifiez et confirmez que la configuration actuelle correspond aux besoins de votre entreprise. S'il s'agit d'une configuration intentionnelle, cette vérification peut être désactivée.	Examiner et décider
Examiner les pages de l'interface utilisateur sans ACL correspondantes	Identifie les pages de l'interface utilisateur qui n'ont pas d'ACL pour cette page de l'interface utilisateur. Les pages de l'interface utilisateur qui n'ont pas d'ACL spécifique utilisent par défaut une ACL de page d'interface utilisateur générique, qui peut accorder l'accès à des utilisateurs non prévus.	Résolution recommandée
Examiner les utilisateurs avec des mots de passe locaux valides	Identifie les utilisateurs avec des mots de passe définis localement. Les utilisateurs avec des mots de passe locaux peuvent interagir avec l'instance via des API en utilisant les informations d'identification locales, même si les connexions locales ne sont pas autorisées. Cette configuration de mot de passe est nécessaire pour que les comptes d'utilisateurs d'intégration fonctionnent correctement. Examinez ces comptes d'utilisateurs pour vérifier que seuls les utilisateurs prévus (tels que les comptes d'intégration) peuvent s'authentifier avec l'authentification locale.	Examiner et décider
Faire pivoter les mots de passe stockés avec des algorithmes de hachage obsolètes	Identifie les comptes d'utilisateurs avec des mots de passe créés dans les versions précédentes de , ServiceNow AI Platform qui ont peut-être utilisé ce qui est maintenant considéré comme un algorithme de hachage hérité ou obsolète.	Résolution recommandée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles des accès Vérifications de l'auditeur (suite)

Nom de vérification	Description	Type de résultat de l'analyse
	Les comptes créés sur les anciennes versions de la plateforme qui n'ont pas fait l'objet d'une rotation des mots de passe peuvent toujours avoir des mots de passe stockés avec un algorithme de hachage hérité. Examinez les comptes identifiés créés, envisagez des réinitialisations de mot de passe.	
Sécurisation des créateurs d'enregistrements	Identifie les créateurs d'enregistrements non sécurisés. Si elles ne sont pas affectées aux rôles appropriés, les utilisateurs non autorisés peuvent y accéder, révélant potentiellement des informations sensibles. Affectez les rôles appropriés aux créateurs d'enregistrements afin de vérifier qu'ils ne sont accessibles qu'aux utilisateurs qui en ont besoin.	Résolution recommandée
Visibilité d'action d'interface utilisateur	Identifie les actions d'interface utilisateur auxquelles un utilisateur sans rôle qui ne dispose pas d'un accès en lecture à la table. Ces utilisateurs peuvent être en mesure de modifier des données dans une table à laquelle ils n'ont pas accès via ces actions d'interface utilisateur. Vérifiez que les actions d'interface utilisateur ne sont disponibles que pour les utilisateurs ayant accès à la table qu'elles affectent.	Résolution recommandée

Traduction automatique

Créer une suite d'analyse

Créez et planifiez une suite personnalisée afin de pouvoir analyser la sécurité de votre instance pour votre organisation.

Avant de commencer

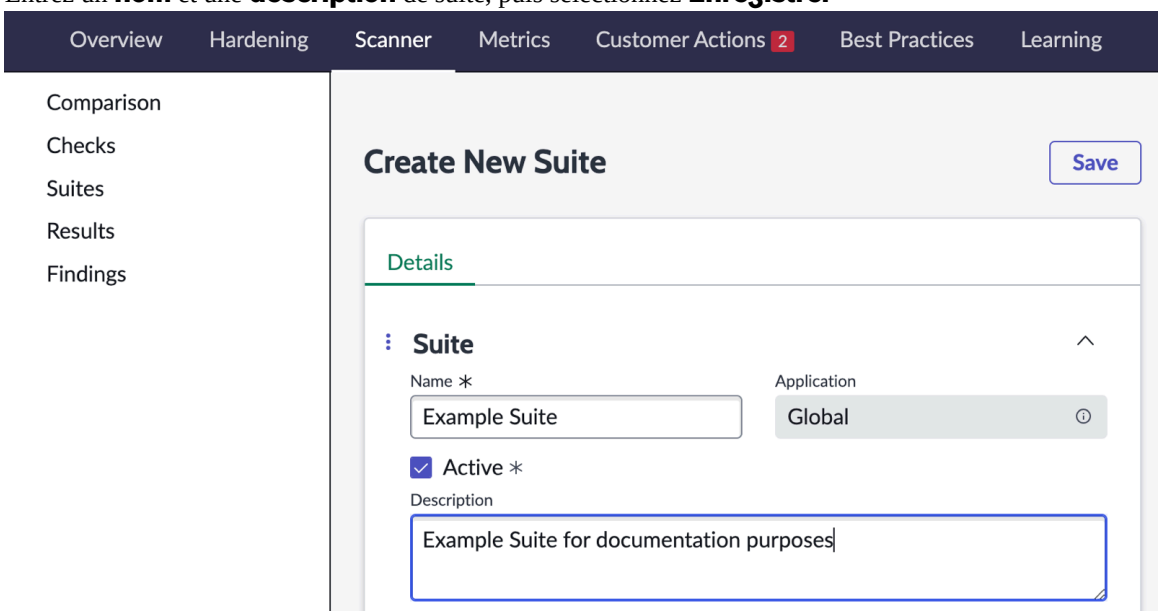
Rôle requis : admin ou sn_vsc.security_center_viewer.

Une suite est une collection de vérifications qui peut être utilisée pour une analyse. Affichez une liste de suites d'analyse organisées dans une table en accédant à **Scanner** > **Suites**. Créez vos propres suites ou, pour utiliser la suite par défaut, Auditeur. Auditor est une suite système de base par défaut qui contient des vérifications de bonnes pratiques de sécurité. Ces vérifications concernent les propriétés système, les modules d'extension et les tables qui peuvent affecter la posture de sécurité de votre instance. Les étapes suivantes montrent comment créer une suite ainsi que les différentes options disponibles pour les configurer.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans Centre de sécurité, sélectionnez l'onglet **Scanner** , puis **Suites** dans le panneau situé à gauche de l'écran.
2. Dans la page **Analyser les suites** , sélectionnez le bouton **Nouveau** .
3. Entrez un **nom** et une **description** de suite, puis sélectionnez **Enregistrer**



Après avoir sélectionné Enregistrer, les options de configuration de la suite s'affichent dans une interface à **onglets**.

4. Sélectionnez l'onglet **Vérifications** .
   Utilisez cet onglet pour ajouter des vérifications à votre suite.
   a. Sélectionnez **Modifier**.
   b. Sélectionnez les vérifications que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour le placer dans votre suite.
   c. **Enregistrer**.
5. Sélectionnez l'onglet **Suites enfants** .
   Utilisez cet onglet pour ajouter des suites enfants. Les suites ajoutées en tant que suites enfants sont également exécutées lorsque cette suite est utilisée dans une analyse.
   a. Sélectionnez **Modifier**.
   b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite enfant.
   c. **Enregistrer**.
6. Sélectionnez l'onglet **Suites parentes** .
   Utilisez cet onglet pour ajouter des suites parentes. Les suites parentes exécutées dans une analyse exécuteront également cette suite.
   a. Sélectionnez **Modifier**.
   b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite parente.
   c. **Enregistrer**.
7. Sélectionnez l'onglet **Calendrier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez cet onglet pour définir le délai d'exécution de votre suite.

a. Sélectionnez **Nouveau**.

b. Entrez les détails de l'analyse planifiée.
Les champs de temps sont au format suivant : heure :minutes :secondes.

c. Enregistrer.

Cloner la suite d'auditeurs des contrôles d'accès

Clonez et personnalisez la suite d'auditeurs de contrôles d'accès par défaut dans votre instance pour créer une nouvelle suite adaptée aux pratiques de sécurité de votre organisation.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La suite d'auditeurs de contrôles d'accès par défaut fournie avec votre instance ne peut pas être modifiée. Toutefois, si vous souhaitez ajouter, supprimer ou modifier des vérifications pour les aligner sur les pratiques de sécurité de votre organisation, vous pouvez dupliquer les suites d'auditeurs de contrôles d'accès. La copie des suites d'auditeurs des contrôles d'accès vous permet de la personnaliser et de créer une suite basée sur la suite par défaut. Les suites d'auditeurs de contrôles d'accès incluent des vérifications liées aux bonnes pratiques de sécurité, couvrant les propriétés système, les modules d'extension et les tables qui ont un impact sur la posture de sécurité de l'instance. Les étapes suivantes montrent comment dupliquer les suites d'auditeurs des contrôles d'accès par défaut pour les adapter aux besoins de votre organisation.

Procédure

1. Accédez à la **Tous** > **Instance Scan** > **Suites**.
2. Sélectionnez **Nouveau** et saisissez un nom pour votre suite, ainsi qu'une description facultative.
3. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
4. Ajoutez les vérifications nécessaires à votre analyse.

   a. Dans l'onglet **Vérifications** , sélectionnez **Modifier**.

   b. Ajoutez les conditions.
   Par exemple, pour ajouter des vérifications d'analyse, appliquez les champs, opérateurs, valeurs et conditions suivants :

   [Catégorie][est][Sécurité] ET [Application][est][Global]

   Par exemple, il doit ressembler à ce qui suit : La catégorie est Sécurité et l'application est Global.

5. Sélectionnez **Exécuter le filtre**.
6. Sélectionnez les vérifications d'analyse que vous souhaitez ajouter de la liste de collecte à la liste de vérification, puis sélectionnez le bouton Ajouter (>).
7. Sélectionnez **Enregistrer**.
   La suite avec vos vérifications personnalisées ajoutées a été créée.
8. Sélectionnez **Exécuter l'analyse de la suite**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher la suite d'auditeurs de contrôles d'accès

Affichez les vérifications disponibles dans les suites d'auditeurs des contrôles d'accès par défaut pour comprendre quelles vérifications sont exécutées lorsque cette suite s'exécute.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les étapes que vous devez suivre pour accéder aux suites d'auditeurs des contrôles d'accès par défaut au sein de votre instance ServiceNow.

Procédure

1. Dans Centre de sécurité, sélectionnez l'onglet **Scanner** , puis **Suites** dans le panneau de gauche.
2. Dans la page **Analyser les suites** , sélectionnez **Auditeur** dans la liste.
3. Pour examiner les vérifications de la suite, sélectionnez l'onglet **Vérifications** .
   Vous devriez voir la liste des 8 vérifications disponibles pour la suite.
4. Sélectionnez le nom d'un chèque que vous souhaitez analyser.
5. Analysez les champs associés à la vérification.

Nom	Description
Nom	Nom de la vérification.
Application	L'application à laquelle la vérification appartient (Centre de sécurité).
Catégorie	Catégorie associée au chèque.
Priorité	Niveau d'urgence.
Version	Numéro de version de la vérification.
Actif	L'état de la vérification, par exemple, actif ou inactif.
Description brève	Un bref résumé de la vérification.
Description	Un résumé plus complet de la vérification.
Détails de la résolution	Atténuation des incidents de sécurité potentiels.
URL de documentation	Liens vers la documentation connexe dans la documentation du produit ou les articles de la base de connaissances.
Condition d'exécution	Conditions qui déclenchent le début des vérifications.
Table	Table à laquelle la vérification appartient.
Conditions	Logique conditionnelle appliquée aux vérifications.
Avancés	Options de configuration avancées.

Replanifier une suite d'analyse

Modifiez le calendrier de vos suites d'analyse en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin, sn_vsc.security_center_viewer

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité**.
2. Dans la section **Outils** , sélectionnez **Scanner de sécurité**.
3. Sélectionnez **Suites** dans le menu situé sur le bord gauche de l'écran.
4. Ouvrez la suite que vous souhaitez replanifier.
5. Sélectionnez l'onglet **Calendrier**.
6. Sélectionnez un calendrier existant ou sélectionnez **Nouveau** pour en créer un.
7. Dans le formulaire **Analyse planifiée** , renseignez les champs selon vos besoins.

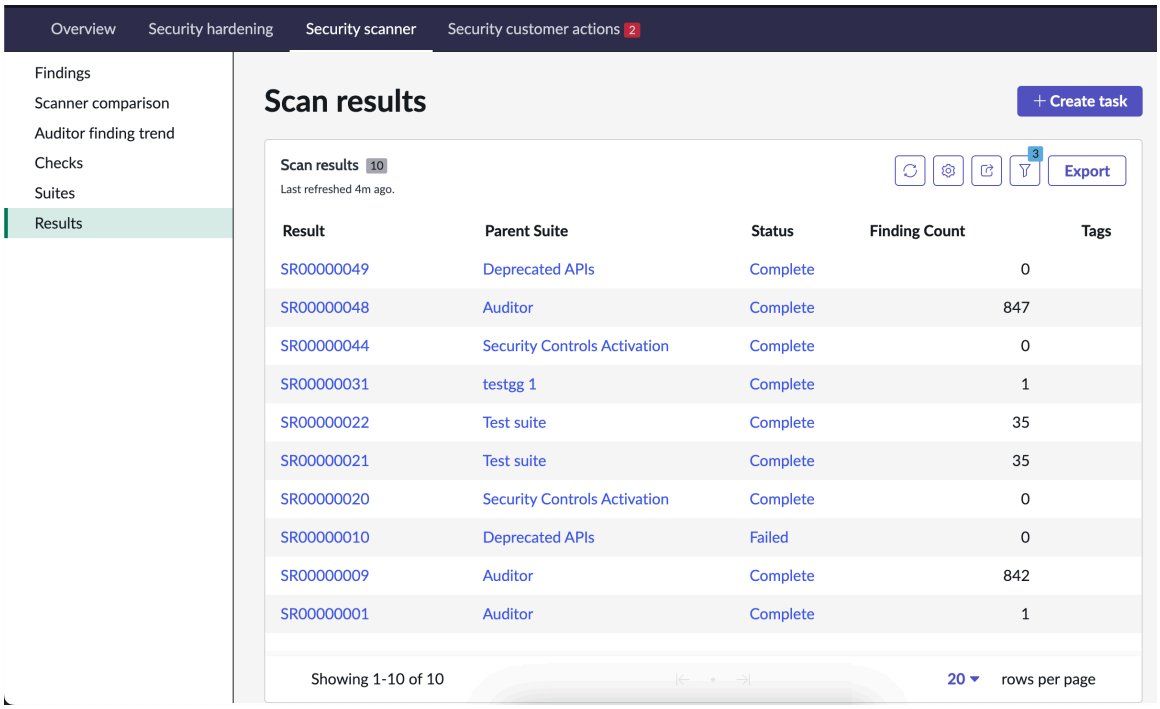
Champ	Description
Nom	Nom du calendrier d'analyse
Exécuter	Sélectionnez la fréquence d'exécution de votre suite. **Remarque :** Des champs supplémentaires apparaîtront pour aider à définir votre calendrier. Ces champs varient en fonction de votre sélection.
Actif	Indique si le calendrier est actif. Les calendriers inactifs ne sont jamais exécutés.
Conditionnel	Sélectionnez cette option pour activer le champ **Condition** , dans lequel vous pouvez définir une condition scriptée pour votre calendrier.
Condition	Une condition scriptée pour votre calendrier. La suite ne s'exécute que lorsque le script est évalué comme `vrai`.
Exécuter en tant que tz	Le fuseau horaire utilisé par le calendrier pour déterminer le moment de l'exécution.

Résultats de l'analyse

Affichez les données relatives aux résultats de votre analyse à partir d'une vue unique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un résultat d'analyse indique l'état et le type d'analyse. Vous pouvez également voir toutes les vérifications exécutées dans le cadre de l'analyse et toutes les autres informations liées à l'analyse, telles que les erreurs et les journaux d'analyse.

Vous pouvez trouver votre tableau de bord des résultats d'analyse en sélectionnant l'onglet **Scanner** dans Centre de sécurité, puis en sélectionnant **Résultats** dans le panneau de gauche. Les résultats de l'analyse sont répertoriés dans la liste **Résultats de l'analyse** . Sélectionnez un résultat à explorer et affichez les détails, qui sont séparés en sections à onglets.

Détails

Vue d'ensemble des résultats de l'analyse, y compris l'état, le type et la durée d'exécution en secondes.

Conclusions de l'analyse

Résultats rencontrés lors de l'exécution des vérifications.

Suites

Affiche les suites exécutées dans le cadre de cette analyse.

Vérifications

Affiche les vérifications exécutées dans le cadre de cette analyse.

Échecs

Affiche les vérifications qui ont échoué pendant l'analyse et la raison de son échec sous la forme d'un message d'erreur.

Journal d'analyse

Affiche les messages émis pendant l'analyse.

Statistiques de l'analyse

Affiche les statistiques relatives à l'analyse.

Cibles

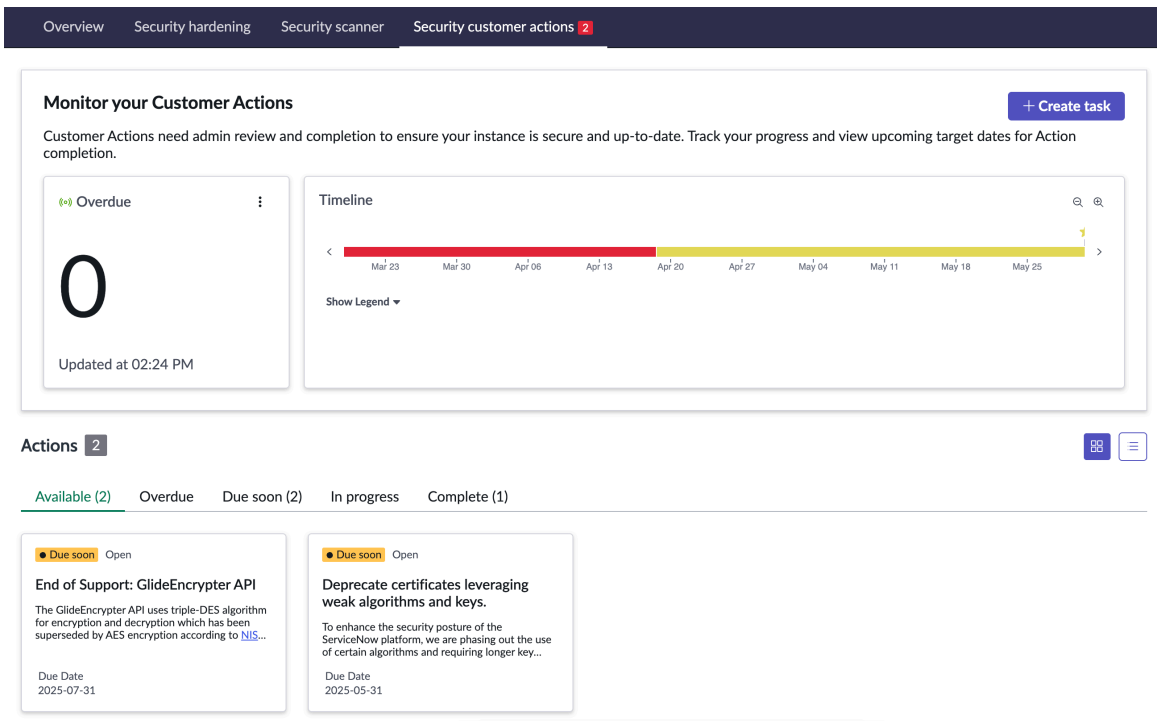
Affiche toutes les cibles sur lesquelles les vérifications ont été exécutées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions du client

Utilisez l'outil Actions du client pour implémenter les mises à jour de sécurité importantes en fonction de votre instance et de la configuration des modules d'extension.



Les actions du client sont des changements recommandés sur une instance qui visent à vous aider à comprendre l'importance des changements liés à la sécurité. Les actions du client implémentées manuellement sont différentes des mises à jour automatiques rendues sur votre instance vers le code ou la fonctionnalité ServiceNow avec des versions de famille ou des correctifs. Implémentez une action client pour éviter d'interférer avec la personnalisation de votre instance.

Sur la page d'accueil Actions des clients, vous pouvez afficher la chronologie des actions des clients afin de pouvoir déterminer par ordre de priorité quand implémenter les étapes. La chronologie de l'exemple ci-dessus montre les actions du client qui sont en retard et celles qui arrivent bientôt à échéance. De plus, vous pouvez suivre la progression de vos actions clients sous l'étiquette Mises à jour. Sélectionnez les onglets afin de voir les actions client disponibles, en retard, bientôt à échéance, en cours ou terminées.

Utilisez le bouton **+Créer une tâche** pour créer une tâche de sécurité afin d'effectuer une action du client. Pour plus de détails, voir Tâches de sécurité.

Démarrer:

- Accédez à cet outil en naviguant jusqu'à **Actions du client** dans Centre de sécurité.
- Les actions du client sont incluses dans l'application Centre de sécurité à partir de Washington DC.

Implémenter les actions du client

Découvrez comment implémenter des actions du client sur votre instance pour renforcer sa posture de sécurité.

Avant de commencer
Rôle requis : admin

Traduction automatique

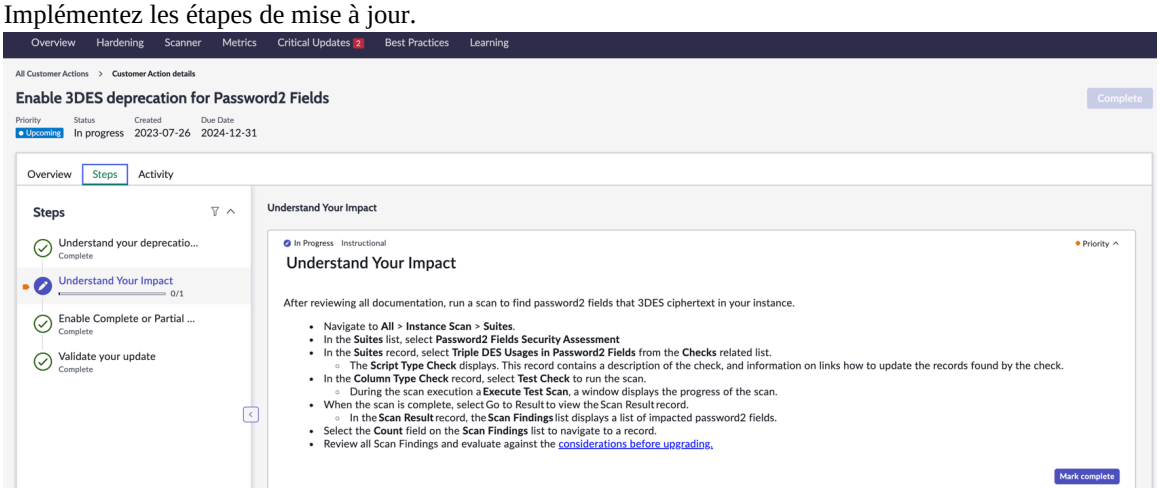
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Actions du client vous fournit des instructions étape par étape sur la façon d'implémenter les changements sur votre instance afin d'augmenter votre posture de sécurité. Customer Actions extrait le contenu pertinent de la documentation produit pour vous guider à chaque étape du processus d'implémentation. Suivez les étapes ci-dessous pour savoir comment implémenter une action du client.

Procédure

1. Accédez à l'application **Actions des clients** .
2. Sélectionnez une action client à implémenter.
   Dans la section **Mises à jour** , l'onglet Disponible répertorie toutes les actions du client sur votre instance. Cliquez sur une action du client sous cet onglet pour afficher les instructions.
3. Lisez la vue d'ensemble pour savoir pourquoi l'action du client est nécessaire et préparer la mise en œuvre des étapes.
   Cliquez sur **Passer à l'étape suivante** pour passer aux détails de l'implémentation.
4. Implémentez les étapes de mise à jour.



   a. Lisez chaque groupe d'instructions et implémentez-les dans votre instance.
   b. Cliquez sur **Marquer comme terminé** lorsque vous avez terminé avec un ensemble d'instructions.
   c. Répétez les étapes a à b jusqu'à ce que vous ayez terminé toutes les étapes de mise à jour.
   d. Cliquez sur **Terminer**.
   L'action du client doit apparaître dans l'onglet **Terminé** .

Afficher les actions du client

Affichez les détails de toutes les activités liées à vos actions client.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les activités sont répertoriées de la plus récente à la plus ancienne afin que vous puissiez d'abord analyser l'activité la plus récente. Chaque mise à jour d'une activité est horodatée, et vous pouvez utiliser la recherche et le filtre pour rechercher des informations spécifiques.

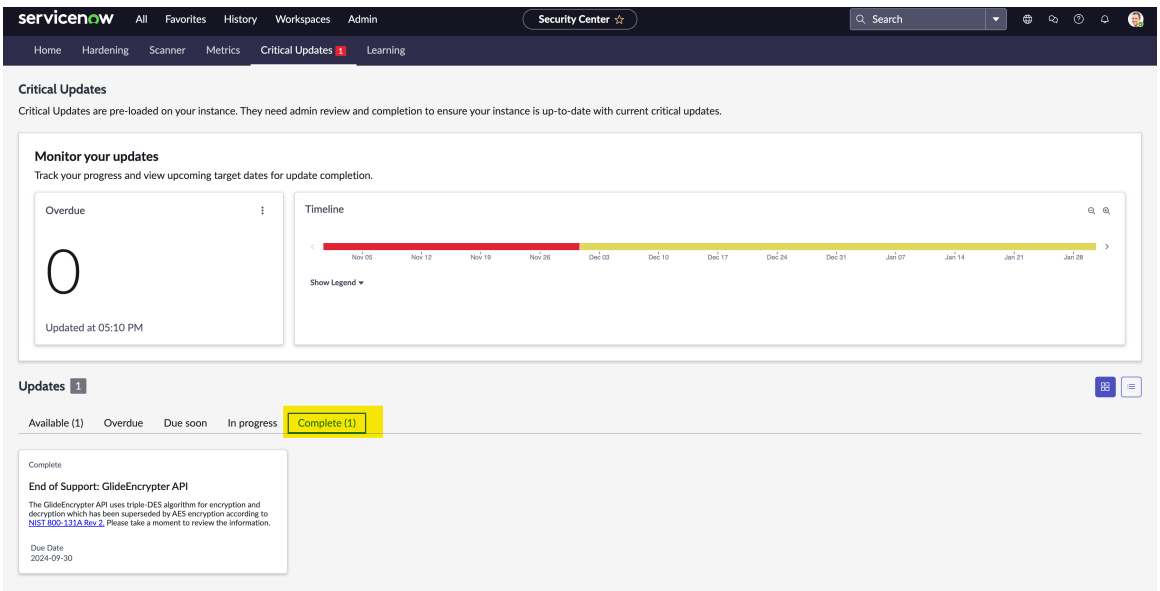
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l’application **Actions des clients** dans le Centre de sécurité.
2. Accédez à l’étiquette**Mises à jour** des actions du client.
3. Cliquez sur un état, puis sélectionnez une action du client dans cet état.

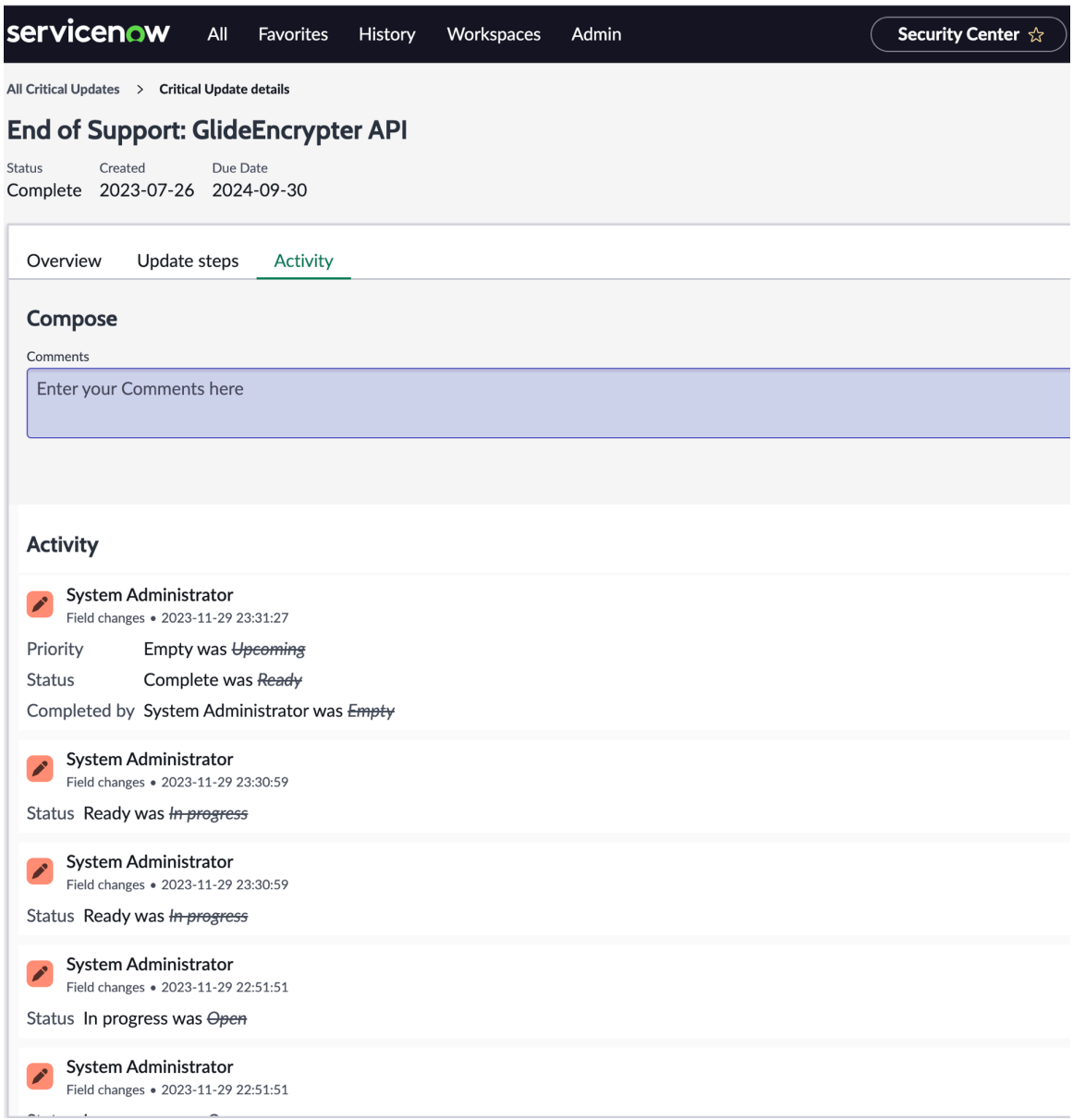
   Dans l’exemple ci-dessous, l’état **Terminé** est sélectionné, puis l’action du client pour **Fin de support : l’API GlideEncrypter** est sélectionnée.



4. Affichez l’activité de votre action client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



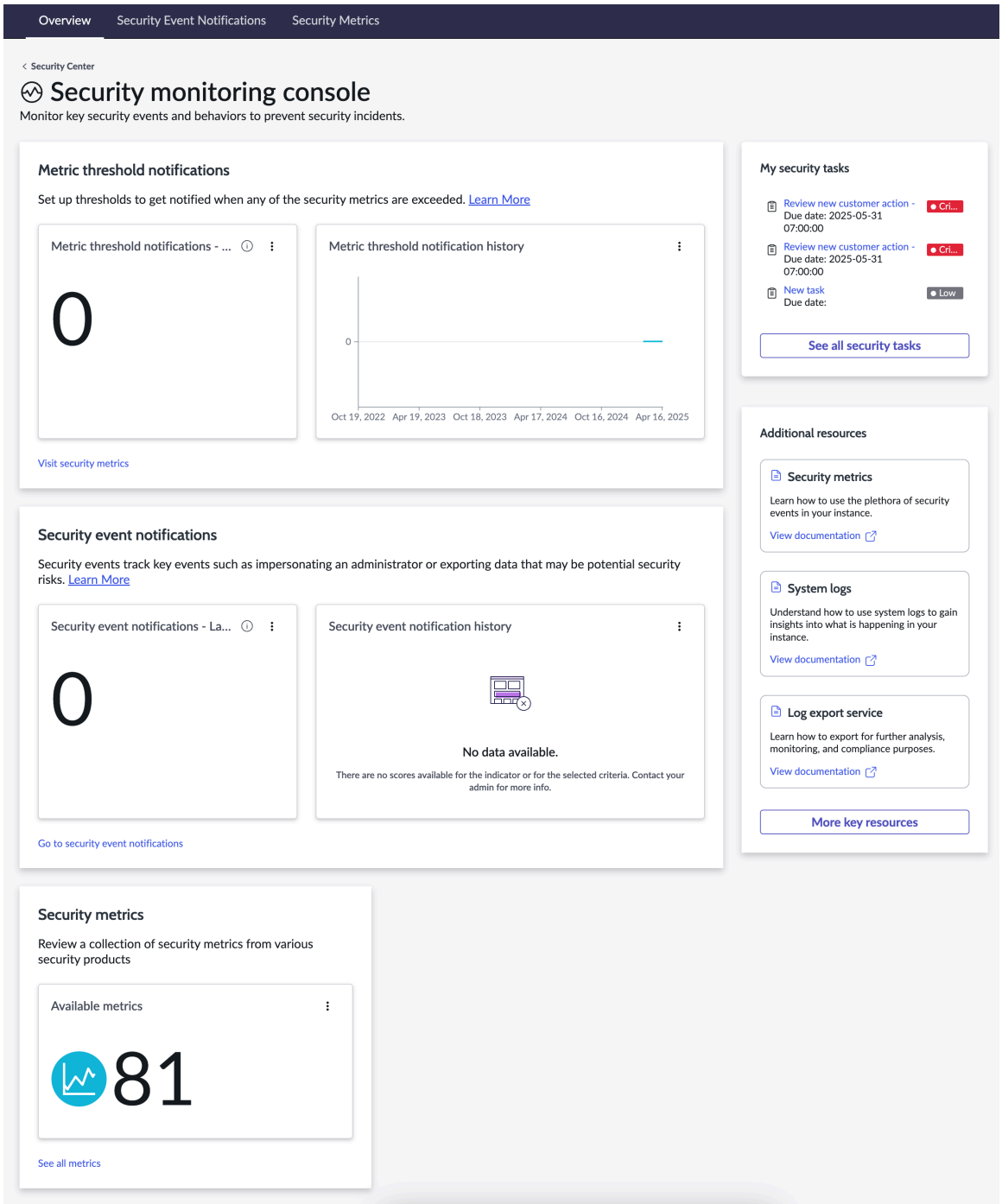
Toute l'activité liée à une action du client est automatiquement enregistrée. De plus, vous avez la possibilité d'ajouter des commentaires supplémentaires aux activités.

Console de surveillance de Sécurité

Supervisez les notifications et les mesures de sécurité pour rester informé des risques de sécurité potentiels sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

La console de surveillance de sécurité est organisée en sections, chacune avec des cartes contenant des informations sur un aspect spécifique de la surveillance de sécurité.

Sélectionnez l'icône d'informations (ⓘ) sur n'importe quelle carte pour obtenir des détails sur ce que chacune représente.

Barre de navigation

Utilisez la barre en haut de la page pour naviguer entre les sections **Vue d'ensemble**, **Notifications des événements de sécurité** et **Mesures de sécurité** .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notifications de seuils de mesure

Découvrez les notifications de seuil de mesure sur votre instance dans le panneau Notifications de seuil de mesure. Les seuils définissent une plage normale de scores pour un indicateur et vous alertent lorsque certains événements se produisent, par exemple lorsqu'un score atteint un niveau record. Ce panneau affiche le nombre de notifications de seuil au cours des sept derniers jours, ainsi qu'un graphique illustrant le nombre de seuils dans le temps.

Sélectionnez l'une des cartes pour ouvrir l'onglet Mesures de sécurité et obtenir plus de détails sur ces notifications.

Notifications des événements de sécurité

Suivez les événements de sécurité tels que les emprunts d'identité ou les exportations de données dans la section Notifications d'événements de sécurité. Ce panneau affiche le nombre d'événements de sécurité au cours des sept derniers jours, ainsi qu'un graphique montrant le nombre au fil du temps.

Sélectionnez l'une des cartes pour ouvrir l'onglet Mesures de sécurité et obtenir plus de détails sur ces notifications.

Mesures de sécurité

Cette section affiche un nombre de mesures de sécurité disponibles sur votre instance. Examiner une collection de mesures de sécurité issues de divers produits de sécurité.

Mes tâches de sécurité

Affichez les tâches de sécurité les plus urgentes qui vous sont affectées. Sélectionnez une tâche pour en afficher les détails, ou sélectionnez **Afficher toutes les tâches de sécurité** pour afficher une liste complète des tâches de sécurité. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Ressources supplémentaires

Utilisez la section Ressources supplémentaires située sur le bord de l'écran pour accéder à la documentation et aux vidéos relatives à l'apprentissage du Centre de sécurité, ainsi qu'à des informations sur la gestion de la sécurité de l'instance.

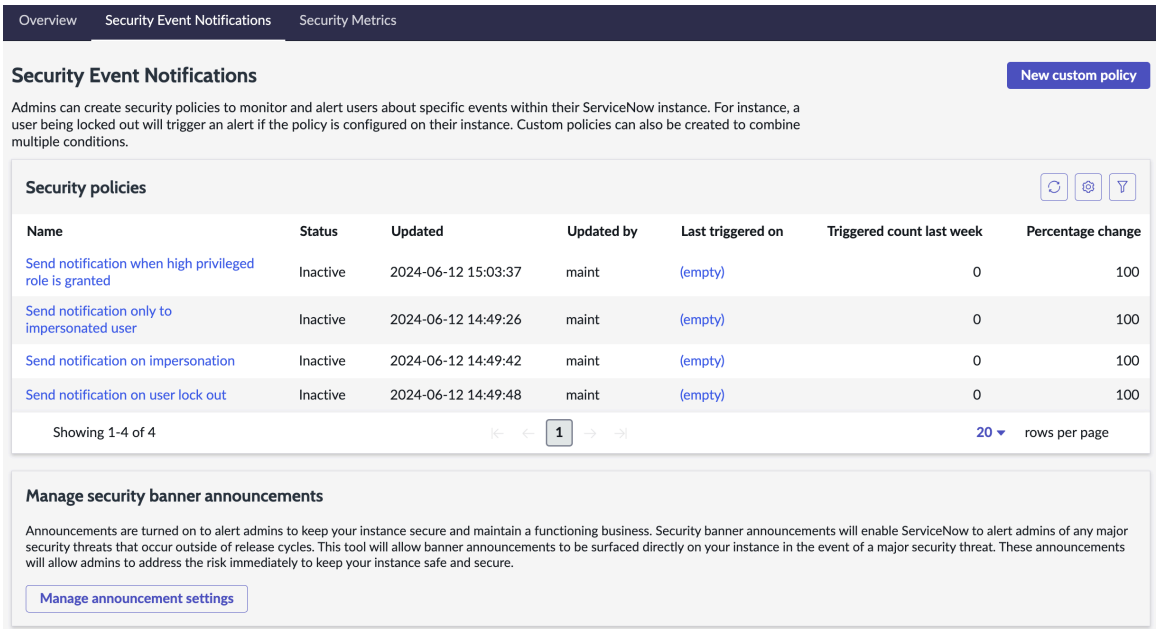
Notifications des événements de sécurité

Affichez, gérez et analysez les politiques de notification d'événements de sécurité par défaut sur votre instance ServiceNow, et accédez à la fonctionnalité permettant de créer des politiques personnalisées.

Accédez aux notifications d'événements de sécurité à partir de la page d'accueil du centre de sécurité en ouvrant la **console de surveillance de sécurité** dans la section **Consoles de sécurité** , puis en sélectionnant l'onglet **Notifications d'événements de sécurité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Personnalisez et créez des politiques de notification qui déclenchent des notifications par e-mail lorsque les utilisateurs effectuent des actions susceptibles de ne pas être sécurisées ou de nécessiter une surveillance de la part de l'administrateur ServiceNow AI Platform .

Les administrateurs peuvent personnaliser les valeurs des politiques par défaut, cloner et modifier les politiques par défaut ou créer leurs propres politiques personnalisées.

Politiques de sécurité

La console Notifications d'événements de sécurité affiche des informations importantes concernant les politiques de sécurité de votre instance. Cette table comprend des colonnes affichant :

Étiquette	Description
Nom	Nom de la politique de notification d'événement de sécurité.
Statut	L'état d'une politique peut être actif ou inactif.
Mis à jour	Date et heure de la dernière mise à jour de la politique.
Mis à jour par	Utilisateur qui a mis à jour une politique.
Dernier déclenchement le	Date et heure de la dernière exécution de la politique.
Nombre de déclenchements la semaine dernière	Nombre de déclencheurs générés par une politique au cours des 7 derniers jours.
Changement de pourcentage	Taux de variation des déclencheurs hebdomadaires, calculé en pourcentage. **Remarque :** Par exemple, si cette politique déclenche en moyenne 5 notifications par semaine et qu'elle s'est déclenchée 10 fois la semaine dernière, cela représenterait une augmentation en pourcentage de 100 %.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez une politique dans la table pour afficher plus de détails, y compris une vue d'ensemble, les paramètres et l'historique des notifications. Sélectionnez le bouton **Nouvelle politique personnalisée** pour créer une politique personnalisée adaptée aux cas d'utilisation de votre organisation.

Gérer les annonces de bannières de sécurité

Sélectionnez **Gérer les paramètres d'annonce** pour contrôler si les administrateurs reçoivent des notifications de bannière sur cette instance. Pour en savoir plus sur ces annonces, reportez-vous à la section Annonces de bannières de sécurité.

Créer des politiques de notification d'événement de sécurité personnalisées

Découvrez comment créer des notifications d'événements de sécurité personnalisées spécifiques aux besoins de votre organisation. Cela vous permet de surveiller les actions effectuées par les utilisateurs et les groupes sur votre instance et de générer des notifications pour détecter les risques de sécurité potentiels.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à l'application Centre de sécurité et sélectionnez **Notifications**.
2. Sélectionnez **Nouvelle politique personnalisée**.
3. Sélectionnez l'un des trois types d'événements qui déclencheront le début de la politique, puis sélectionnez **Créer**.
4. Configurez la politique.
   Reportez-vous à la section Configurer les préférences pour les politiques de notification d'événements de sécurité pour savoir comment configurer votre nouvelle politique de notification d'événement de sécurité personnalisée.

Modifier les politiques de notification d'événement de sécurité

Découvrez comment modifier les paramètres de vos politiques de notification d'événements de sécurité.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la page d'accueil des **notifications** d'événements de sécurité et sélectionnez l'une des stratégies que vous souhaitez modifier.

   Remarque :
   Vous ne pouvez pas modifier la logique de déclenchement ou de condition pour les politiques par défaut. Pour modifier ces paramètres, vous devez d'abord dupliquer la stratégie, ce qui peut être fait en sélectionnant la flèche vers le bas en regard de **Mettre à jour**, puis en sélectionnant **Dupliquer**.

2. Sélectionnez **les paramètres de politique** pour modifier les paramètres.
3. Sélectionnez **Mettre à jour** pour enregistrer vos changements.
4. **Facultatif :** Sélectionnez **Désactiver** jusqu'à ce que vous soyez prêt à commencer à déclencher des notifications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Facultatif :** Commencez à déclencher des notifications en sélectionnant **Activer**.
   Reportez-vous à la section Configurer les préférences pour les politiques de notification d'événements de sécurité pour savoir comment configurer votre nouvelle politique de notification d'événement de sécurité personnalisée.

Configurer les préférences pour les politiques de notification d'événements de sécurité

Découvrez comment personnaliser les politiques de notification d'événements de sécurité pour Centre de sécurité qu'elles soient en adéquation avec les besoins spécifiques de votre organisation.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La page **Paramètres de la politique** est l'endroit où vous pouvez personnaliser les paramètres d'une politique de notification d'événement de sécurité. Ici, vous pouvez ajuster les options liées au moment d'exécution de la politique, à la logique conditionnelle et aux notifications envoyées.

Procédure

1. Dans Centre de sécurité, sélectionnez **Notifications**.
2. Dans la table Politiques de sécurité, sélectionnez une stratégie de notification d'événement de sécurité que vous souhaitez configurer.
   Par exemple, **envoyer une notification lorsque le rôle hautement privilégié est accordé**.
3. Sélectionnez **Paramètres de politique**.
4. Configurez les paramètres de stratégie.

Options de configuration des paramètres de politique

Étiquette	Ce qu'il faut configurer
Quand exécuter	**Déclencheur** : l'événement qui lance la politique.
Conditions	La logique conditionnelle et les conditions à appliquer à vos stratégies. ○ **Logique de condition** : deux options ▪ **Toutes les conditions doivent être remplies pour déclencher cette politique** : toutes les conditions doivent être valides pour que la politique envoie des notifications. ▪ **L'une des conditions suivantes doit être remplie pour déclencher cette politique** : des notifications seront envoyées si l'une des conditions est valide. ○ **Ajouter une condition** : sélectionnez Ajouter une condition et fournissez-lui les valeurs appropriées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette	Ce qu'il faut configurer
	Vous pouvez supprimer une condition en sélectionnant **Supprimer la condition**.
Notifications	Le corps de l'e-mail et les destinataires de l'e-mail : ○ **Notification** : sélectionnez l'un des modèles de notification prédéfinis. Consultez Créer un e-mail personnalisé pour les notifications d'événements de sécurité pour plus d'informations. ○ **Ajouter une notification** : sélectionnez Ajouter une notification. ○ **Groupes** : sélectionnez le groupe qui doit recevoir la notification. ○ **Utilisateurs** : sélectionnez les utilisateurs qui doivent recevoir la notification. Vous pouvez supprimer une notification en sélectionnant **Supprimer la notification**.

Remarque :
Si vous souhaitez rendre une politique inactive, sélectionnez **Désactiver**. Si vous souhaitez répliquer une politique, sélectionnez la flèche vers le bas en regard du bouton **Mettre à jour** (bouton



).

5. Sélectionnez **Mettre à jour** pour enregistrer vos paramètres.

Créer un e-mail personnalisé pour les notifications d'événements de sécurité

Découvrez comment créer un e-mail personnalisé pour les notifications d'événements de sécurité en configurant de nouvelles notifications, en définissant des déclencheurs, en définissant des destinataires et en élaborant du contenu d'e-mail avec des champs d'événements dynamiques.

Avant de commencer
Rôle requis : admin

Procédure

1. Sélectionner **Notifications système** > **Notification**.
2. Sélectionnez **nouveau**.
3. Entrez un **nom** pour le champ de notification.
4. Sélectionnez le champ en regard de la **table** et saisissez notification de politique de sécurité (*sn_vsc_security_policy*).
5. Configurez le nouvel enregistrement.
   Il y a trois onglets dans l'enregistrement qui doivent être configurés : **Quand envoyer**, **Qui recevra** et **Ce qu'il contiendra**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
Quand envoyer	Sélectionnez le champ en regard de l'étiquette **Envoyer quand** et sélectionnez **Déclenché**.
Qui recevra	○ Sélectionnez l'icône locale en regard de **Utilisateurs/groupes dans les champs**, puis sélectionnez **Utilisateurs** et **Groupes**. Sélectionnez l'icône **Ajouter un élément** (>) pour déplacer les champs dans le champ de texte **Sélectionné** . ○ Cliquez avec le bouton droit sur la bannière d'en-tête d'enregistrement, puis sélectionnez **Enregistrer**.)

Ce qu'il contiendra	Créez un modèle d'e-mail.
	Consultez Create an email template pour plus d'informations.
	Entrez les champs de l'événement dans le **message HTML**. Cela peut être fait en utilisant le ${event_id.FIELD_NAME}. Voici un exemple :
	`Role: ${event_id.role.URI_REF}`
	`Granted to: ${event_id.granted_to.URI_REF}`
	`Granted by: ${event_id.user.URI_REF}`
	`Logged at: ${event_id.sys_created_on}`
	`Security Center Notification: ${execution.policy.name}`

6. Sélectionnez **Soumettre**.
7. Ajoutez une notification personnalisée au modèle d'e-mail dans les notifications d'événements de sécurité.
   a. Dans Centre de sécurité, sélectionnez **Notifications** > **Paramètres de politiques**.
   b. Accédez à l'étiquette **Notifications** .
   c. Entrez le nom de la notification personnalisée que vous avez créée dans le champ **Notification** .

Historique des notifications d'événements de sécurité

Explorez l'historique complet des notifications d'événements de sécurité sur votre instance.

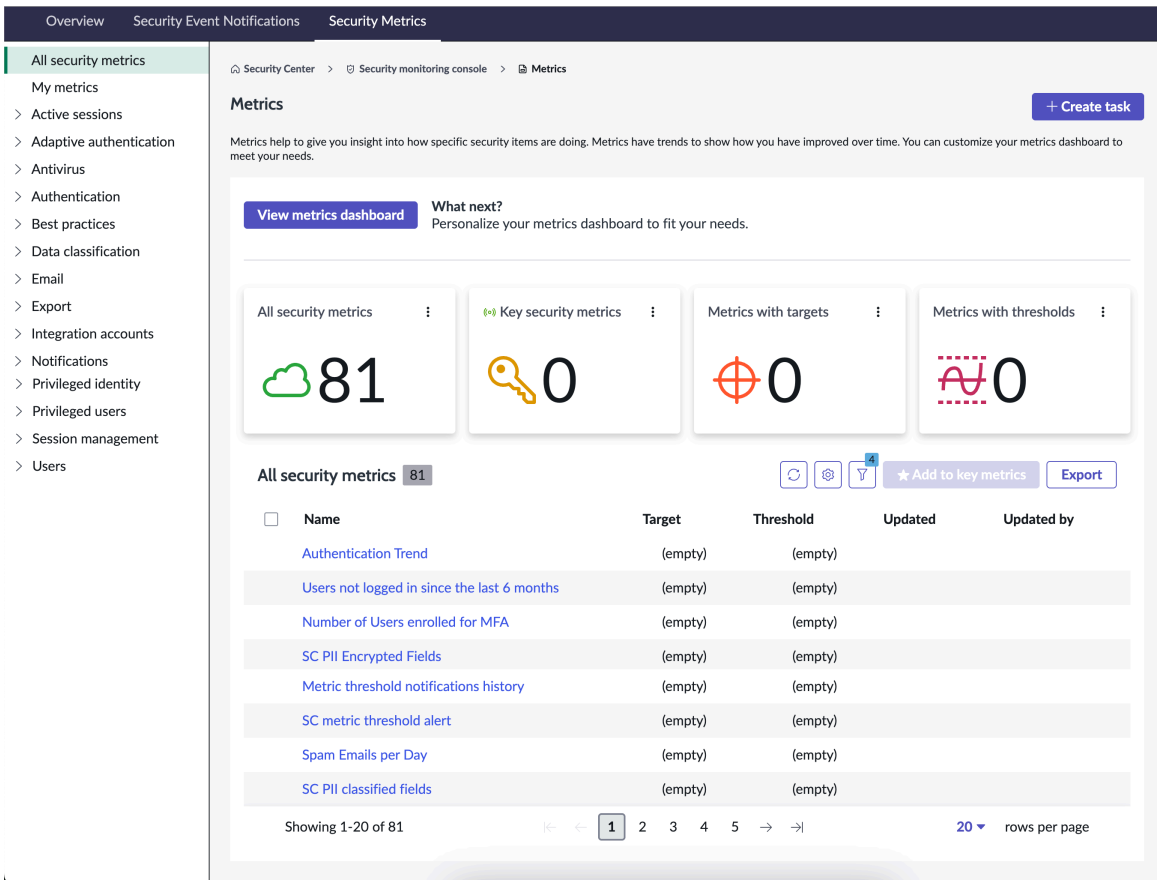
La page **Notifications** fournit une vue d'ensemble de l'historique des notifications pour toutes les politiques de notification d'événement de sécurité sur votre instance. Vous pouvez afficher les données dans des graphiques, les présenter graphiquement et appliquer des fonctionnalités d'analyse des performances telles que les cibles, les seuils et les signaux KPI. Vous pouvez également afficher les données sous forme de tableau, ce qui vous permet d'utiliser des fonctionnalités standard telles que la recherche, le tri, le filtrage et l'interrogation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de sécurité

Surveillez plus de 50 mesures de sécurité différentes pour identifier les menaces de sécurité potentielles ou les comportements non sécurisés. Définissez des seuils pour les notifications par e-mail, visualisez et analysez les données de plusieurs façons. Exportez les données ou créez des tableaux de bord avec les mesures les plus importantes pour votre organisation.



Accéder aux mesures de sécurité dans Centre de sécurité en sélectionnant **Surveillance de sécurité** dans la section Outils. Sélectionnez ensuite la carte **Mesures de sécurité** .

Tableau de bord Toutes les mesures de sécurité

Affichez des mesures telles que les échecs de connexion, les exportations, les emprunts d'identité et plus encore à l'aide de ce tableau de bord. Les cartes situées au-dessus de la liste indiquent le nombre de mesures qui correspondent à des critères spécifiques répertoriés sur la carte. Sélectionnez l'une de ces cartes pour filtrer la liste afin d'afficher uniquement les mesures qui correspondent aux critères.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Tableau de bord de mes mesures

Il s'agit d'un tableau de bord personnalisable qui affiche des informations sur les mesures qui vous intéressent le plus. Sélectionnez **Modifier** pour personnaliser votre tableau de bord en ajoutant des visualisations, des filtres, des en-têtes, des images, du texte enrichi et des listes. Pour en savoir plus sur les différentes façons de personnaliser votre tableau de bord, reportez-vous à la rubrique Dashboards in Platform Analytics .

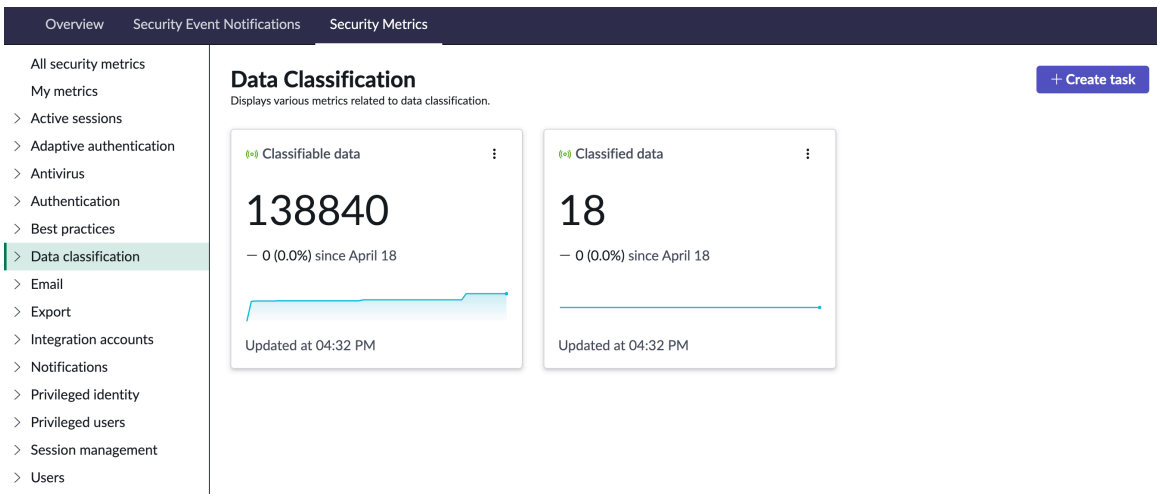
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Volet de navigation des mesures

Le volet de navigation sur le bord de l'écran affiche les mesures de votre instance. Sélectionnez **Toutes les mesures de sécurité** pour afficher toutes les mesures dans une seule liste. Sélectionnez l'un des éléments sous **Toutes les mesures de sécurité** l'entrée pour parcourir les mesures organisées par catégorie.

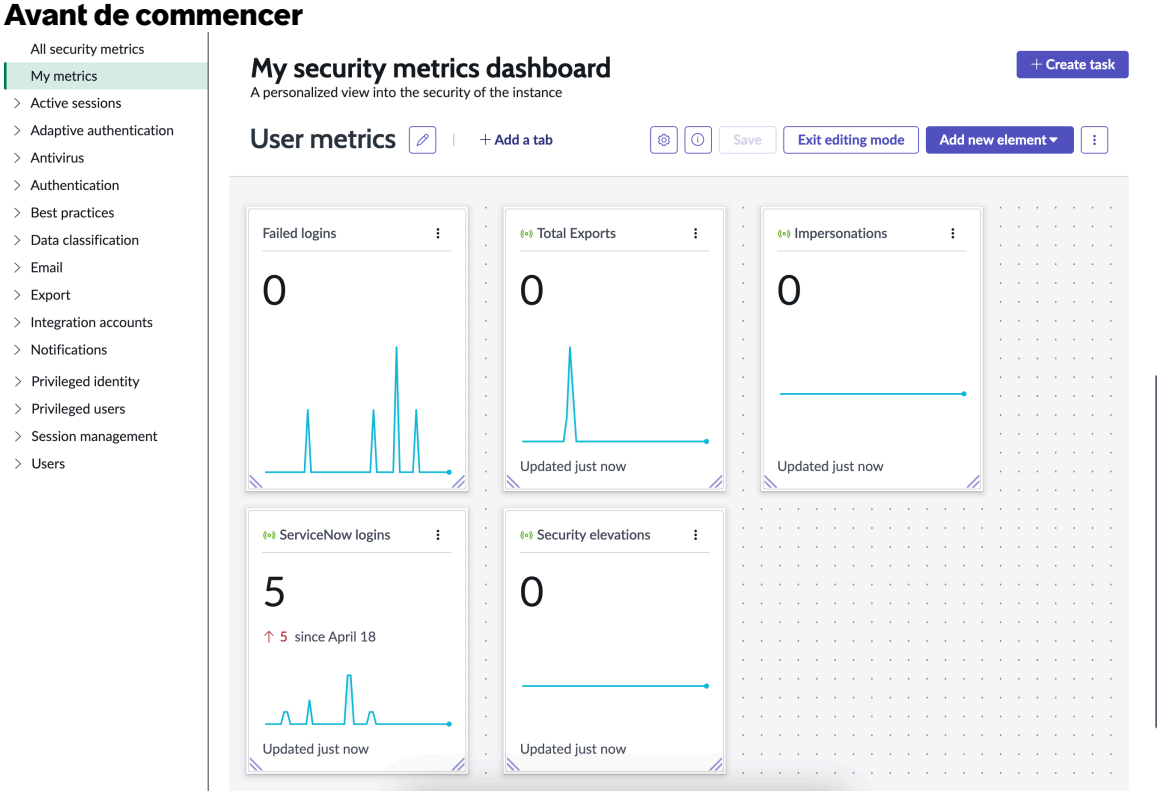
Chaque catégorie affiche un tableau de bord similaire au **tableau de bord Sécurité Mes mesures**, avec des cartes pour les mesures de cette catégorie.



Personnaliser le tableau de bord Mes mesures de sécurité

Découvrez la flexibilité du tableau de bord Mes mesures de sécurité, qui peut être personnalisé avec des mesures provenant de diverses sources telles que des graphiques et des tableaux. Adaptez le tableau de bord aux besoins spécifiques de votre organisation.

Avant de commencer



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour personnaliser le tableau de bord Mesures de sécurité, confirmez que vous êtes dans le périmètre de l'application Centre de sécurité. Pour basculer vers ce périmètre, sélectionnez **Sélecteur d'application** > **Périmètre de l'application**et le type Centre de sécurité.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Implémenter et personnaliser le tableau de bord Mes mesures de sécurité. Ajoutez des mesures et du contenu à votre tableau de bord à partir de diverses sources, telles que des graphiques et des diagrammes générés à partir d'un rapport. Découvrez les étapes requises pour ajouter un onglet à votre tableau de bord afin de pouvoir le personnaliser en fonction des besoins de votre organisation.

Procédure

1. Accéder aux mesures de sécurité dans Centre de sécurité en sélectionnant **Surveillance de la sécurité** dans la section Outils et en sélectionnant la carte **Mesures de sécurité** .
2. Entrez en mode d'édition en sélectionnant **Modifier**.
3. Créez un onglet en sélectionnant **+Ajouter un onglet**.

   Remarque :
   Vous pouvez également ajouter un nouvel onglet en sélectionnant l'icône **plus (+)** en regard d'un onglet existant.

4. Modifiez le titre de votre nouvel onglet en sélectionnant l'icône en forme de crayon et en saisissant un nom.
5. Ajoutez un élément à votre onglet en sélectionnant **Ajouter un nouvel élément**.
6. Sélectionnez **Enregistrer**.
7. **Facultatif :** Pour partager le tableau de bord avec des utilisateurs, des groupes et des rôles de votre organisation, sélectionnez **Menu Plus d'actions** > **Partager**.
   a. Entrez le nom d'un utilisateur auquel accorder l'accès.
   b. Sélectionnez **Confirmer**.

Configurer les mesures de sécurité pour envoyer un e-mail lorsque des seuils sont déclenchés

Découvrez comment configurer les mesures de sécurité de sorte que votre instance génère une notification par e-mail lorsqu'un seuil est déclenché.

Avant de commencer

Rôle requis : admin

Procédure

1. Dans le Centre de sécurité, accédez aux **mesures**.
2. Sélectionnez une mesure pour laquelle vous souhaitez définir un seuil dans votre organisation.

   Example
   Pour gérer les échecs de connexion, vous pouvez définir un seuil. Lorsque le nombre d'échecs de connexion atteint ce seuil, les administrateurs ou les experts en sécurité de votre organisation en sont informés. La mesure de sécurité appropriée à cibler dans ce cas est **utilisateurs** > **Échecs de connexion**.
3. Sélectionnez l'icône **Seuils** .
4. Sélectionnez l'icône **plus (+)** sur le panneau des seuils pour configurer le formulaire.
   Les options disponibles permettent de définir la visibilité, le type de seuil et la valeur de seuil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Pour plus de visibilité, sélectionnez **Pour tout le monde** si vous souhaitez que tout le monde reçoive la notification, ou **pour moi** si vous souhaitez uniquement recevoir une notification.

b. Dans Type **de seuil**, sélectionnez **Tout le temps Élevé**.
Ce champ déclenche la notification de seuil.

> **Remarque :**
> Une valeur de seuil ne doit être saisie que lorsque le **type de seuil** est défini sur **Inférieur** ou **supérieur à**.

5. Sélectionnez **Enregistrer** pour créer le seuil.
Ensuite, la notification doit être configurée.
6. Sélectionnez **tout**, puis saisissez **une notification système**.
7. Accédez à la **E-mail** > **notifications**.
8. Dans la colonne **nom** , entrez `*pa thre`.
Les notifications de seuil sont basées sur les événements et sont configurées dans la table Notification de seuils PA.
9. Sélectionnez **Notification de seuils PA**.
Il y a trois onglets dans les résultats :
   - Quand envoyer : spécifie ce qui doit se produire pour envoyer la notification par e-mail. Dans cet exemple, une fois que le seuil que vous avez défini précédemment est atteint, l'e-mail est déclenché.
   - Qui recevra : spécifie quels utilisateurs reçoivent la notification. Vous pouvez ajouter des utilisateurs et des groupes.
   - Ce qu'il contiendra : spécifie l'action des scripts qu'un utilisateur peut modifier pour personnaliser le message que les utilisateurs et le groupe recevront. Pour en savoir plus sur la création d'actions de script, reportez-vous à la section Script actions .

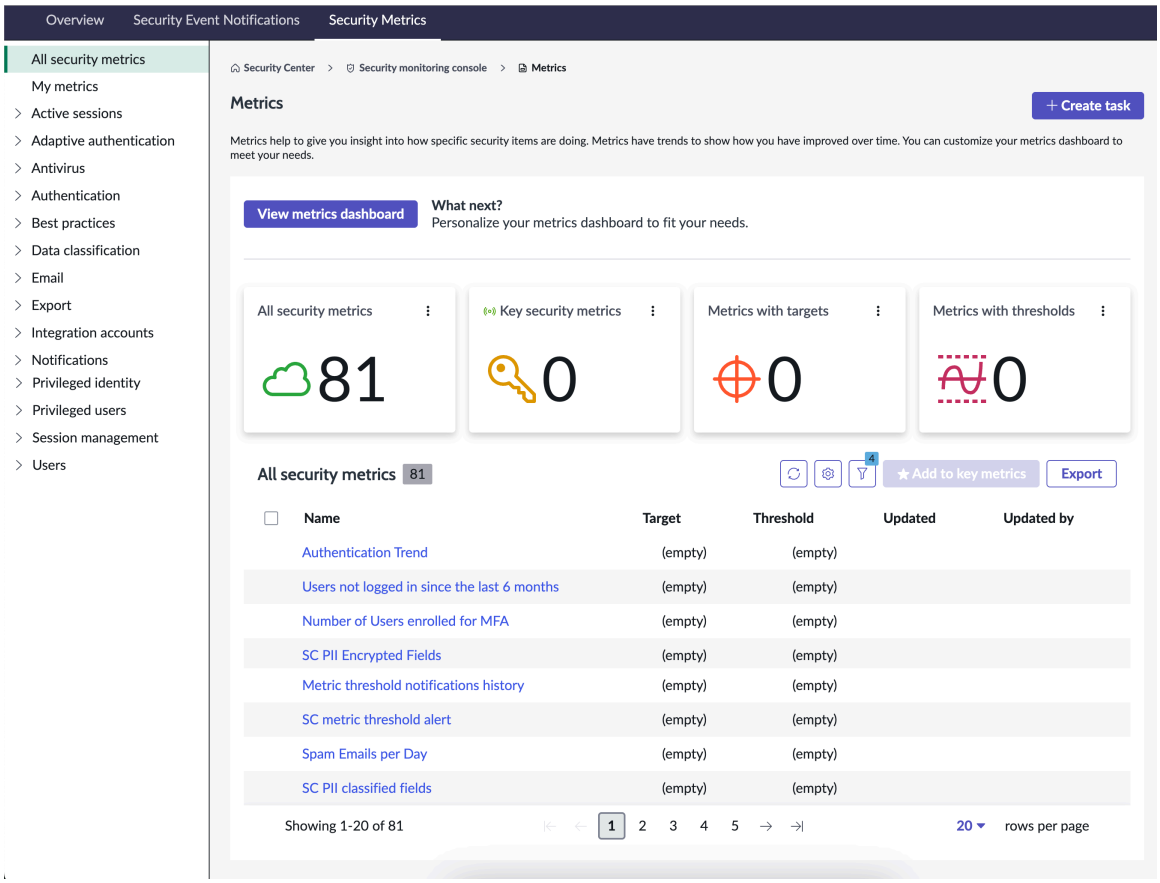
Toutes les mesures de sécurité

Accédez à **Toutes les mesures de sécurité** pour afficher une table contenant les données relatives aux mesures de sécurité de votre instance.

Accédez à la liste de toutes les mesures de sécurité d'une liste filtrable en accédant au tableau de bord des mesures de sécurité et en sélectionnant l'option **Toutes les mesures de sécurité** dans la liste de gauche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Sélectionnez n'importe quel élément de la liste pour afficher les détails de chaque mesure.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Sessions actives

Affichez la ligne de tendance des utilisateurs actifs sur le ServiceNow AI Platform.

Cette page affiche les cartes contenant des informations sur les mesures liées aux sessions actives. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Sessions utilisateur : mesures liées aux sessions utilisateur actives sur votre instance.
- Sessions des utilisateurs privilégiés : mesures relatives aux utilisateurs privilégiés ou à ceux auxquels des rôles supplémentaires ont été affectés.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Mesures de sécurité pour l'authentification adaptative

Utilisez des politiques d'authentification pour évaluer les demandes d'authentification et refuser ou autoriser l'accès à votre instance en fonction des conditions de politique spécifiées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les métriques d'authentification adaptative vous permettent de surveiller la façon dont l'authentification adaptative est utilisée sur votre instance. Affichez un résumé de toutes vos mesures sur l'authentification adaptative, des mesures individuelles telles que les taux de résultats de politique ou les adresses IP refusées. Le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) pour l'authentification adaptative doit être disponible dans votre instance pour cette page. Vous devez activer la politique d'authentification pour voir les mesures. Voir Activer l'authentification adaptative et Configurer les propriétés d'authentification adaptative pour plus de détails.

Remarque :
Cette fonctionnalité a été publiée avec la version 1.2.

- Taux de résultats de la politique : tous les événements d'authentification adaptative réussis et échoués.
- Distribution d'échecs d'événements : tous les événements ayant échoué pour chaque type d'événement.
- Distribution de la réussite d'événement : les événements réussis associés à chaque type d'événement.
- Adresses IP refusées : le nombre d'adresses IP bloquées par l'instance, ainsi que leurs données associées.
- Connexions des utilisateurs authentifiés : nombre d'événements comptés pour chaque type d'événement, à l'exclusion de l'événement de préconnexion.
- Connexions des utilisateurs de l'API : nombre d'événements associés aux politiques d'authentification d'API pour chaque type d'événement.
- Tendance en matière d'authentification : nombre total d'événements enregistrés.
- Utilisateurs authentifiés : nombre d'utilisateurs comptés pour chaque type d'événement, à l'exclusion de l'événement de préconnexion.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Antivirus

Affiche la tendance à laquelle les événements se produisent sur les fichiers potentiellement infectés. Voyez quand ils sont détectés, placés en quarantaine, restaurés ou supprimés.

Cette page affiche des cartes contenant des informations sur les mesures liées à l'activité antivirus sur votre instance. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Fichiers en quarantaine : nombre de fichiers qui contiennent potentiellement des programmes malveillants.
- Fichiers téléchargés : le nombre de fichiers téléchargés.
- Fichiers restaurés : nombre de fichiers qui ont été restaurés.
- Fichiers supprimés : le nombre de fichiers supprimés.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Authentification

Affichez les tendances des mesures liées aux schémas d'authentification, telles que l'utilisation de l'authentification multifacteur (MFA), les comptes de service Web et l'utilisation des scanners biométriques.

Cette page affiche les cartes contenant des informations sur les mesures liées à l'authentification. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Utilisateurs inscrits pour MFA
- Utilisateurs utilisant la MFA
- Utilisateurs non MFA aux privilèges élevés
- Utilisateurs de la MFA actifs
- Utilisateurs de MFA bloqués
- Compte de service web uniquement
- Certificats X509 arrivant à expiration dans 30 jours
- Utilisateurs clés de scanners biométriques/matériels
- API REST sans politique d'accès
- Comptes d'intégration sans marqueur d'accès au service Web uniquement activé

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Classification des données

Accédez aux mesures de sécurité pour la classification des données sur votre instance ServiceNow.

La classification des données vous permet d'appliquer des étiquettes de classification des données à des entrées de dictionnaire existantes dans n'importe quelle table. Ces étiquettes permettent de fournir une visibilité sur les types de données hébergées dans vos instances. Utilisez ces classifications pour vous conformer aux lois sur la confidentialité et aux exigences réglementaires du secteur.

Voir la classification des données pour plus d'informations.

- **Données classifiables** : tables ou colonnes qui peuvent être classées.
- **Données classifiées** : entrées de dictionnaire, tables ou colonnes classifiées.

Les données sont affichées graphiquement dans un graphique personnalisable qui fournit une analyse détaillée telle que la définition de cibles, de seuils, de tendances, de statistiques ou de prévisions. Les données sont également organisées sous forme d'enregistrements dans une table. Consultez Analytics Hub pour plus d'informations.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Mesures d'authentification

Affichez les mesures liées à l'authentification sur votre instance à partir d'un tableau de bord.

Cette page affiche les cartes contenant des informations sur les mesures liées à l'authentification. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Utilisateurs inscrits pour la MFA : nombre total d'utilisateurs inscrits pour utiliser la MFA.
- Utilisateurs utilisant le contournement MFA : nombre total d'utilisateurs qui contournent l'authentification multifacteur.
- Utilisateur non MFA aux privilèges élevés : nombre total d'utilisateurs aux privilèges élevés qui n'utilisent pas la MFA.
- Utilisateurs de MFA actifs : nombre total d'utilisateurs de MFA actifs sur votre instance.
- Utilisateurs MFA bloqués : nombre total d'utilisateurs MFA qui sont verrouillés sur votre instance.
- Utilisateur de compte de service Web : nombre total d'utilisateurs avec un compte de service Web uniquement.
- Certificats X509 arrivant à expiration : nombre total de certificats X509 venant à expiration dans les 30 prochains jours.
- Utilisateurs de scanner biométriques/clé matérielles : nombre total d'utilisateurs qui se connectent avec un scanner biométrique ou une clé matérielle.
- Politique sans accès des API REST : nombre total d'utilisateurs qui se connectent sans la politique d'accès des API REST.
- Comptes d'intégration sans accès au service Web uniquement Marqueur activé : nombre total d'utilisateurs connectés sans comptes d'intégration Marqueur d'accès au service Web uniquement activé.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

E-mail

Affiche les données relatives aux courriers indésirables reçus en externe.

La page affiche une carte qui affiche une ligne de tendance des spams, représentant le nombre de courriers indésirables reçus par jour.

Sélectionnez la carte pour afficher des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exporter

Découvrez les données qui sont couramment exportées et quels utilisateurs effectuent l'exportation.

Cette page affiche des cartes contenant des informations sur les mesures liées à l'exportation. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Exportations totales : nombre total d'enregistrements de table exportés par l'utilisateur.
- Exportations classées : nombre total d'enregistrements de table exportés, résumé selon la classification des données qui leur est affectée.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Comptes d'intégration

Affichez les tendances relatives aux comptes d'intégration créés sur le ServiceNow AI Platform.

Cette page affiche les cartes contenant des informations sur les mesures liées aux comptes d'intégration créés sur le ServiceNow AI Platform. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Total des comptes d'intégration : tendances relatives aux comptes d'intégration sur votre instance.
- Comptes d'intégration actifs : tendances relatives aux comptes d'intégration actifs sur votre instance.
- Comptes d'intégration inactifs : tendances du nombre total de comptes d'intégration inactifs sur votre instance.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Identité privilégiée

Analyser les données relatives aux mesures pour les utilisateurs ayant une identité privilégiée.

Cette page affiche des cartes contenant des informations sur les mesures relatives aux utilisateurs d'identité privilégiés et à leur activité sur votre instance. Chaque carte affiche une ligne de tendance pour les mesures suivantes :

- Connexions d'administration : nombre total de connexions avec des utilisateurs du rôle administrateur.
- Emprunt d'identité : nombre total d'emprunts d'identité effectués par les utilisateurs disposant du rôle emprunteur d'identité.
- Élévation : nombre total d'élévations de sécurité effectuées par les utilisateurs disposant du rôle security_admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connexions ServiceNow : nombre total de connexions par les employés de ServiceNow.
- Utilisateurs administrateurs ajoutés : Nombre total d'utilisateurs ayant reçu le rôle administrateur.

Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Utilisateurs privilégiés

Affichez la ligne de tendance des utilisateurs privilégiés (actifs et inactifs) et leur activité sur le ServiceNow AI Platform.

La section Vue d'ensemble Utilisateurs privilégiés affiche la ligne de tendance des utilisateurs privilégiés (actifs et inactifs) et leur activité sur le ServiceNow AI Platform. Les utilisateurs privilégiés sont des utilisateurs auxquels des rôles supplémentaires ont été affectés par des administrateurs pour accéder aux fonctionnalités telles que Paramètres de sécurité élevée, Importation et Utilisateurs du portail.

Vous trouverez ci-dessous une explication des utilisateurs privilégiés :

- Total des utilisateurs : nombre total d'utilisateurs sur votre instance.
- Utilisateurs actifs : nombre total d'utilisateurs qui ont initié des sessions sur votre instance.
- Utilisateurs inactifs : utilisateurs qui ne se sont pas récemment connectés à votre instance.
- Utilisateurs inactifs qui ne sont pas bloqués : utilisateurs qui ne se sont pas récemment connectés mais qui ont toujours accès à leur compte.
- Utilisateurs bloqués : utilisateurs qui ne sont pas autorisés à s'authentifier dans leur compte.
- Nouveaux utilisateurs : utilisateurs qui ont récemment été ajoutés à votre instance.
- Connexions réussies : utilisateurs qui se sont connectés avec succès.
- Échecs de connexion : tentatives de connexion infructueuses.
- Connexions locales non protégées par MFA : utilisateurs qui se sont connectés sans MFA.
- Utilisateurs qui ne se sont jamais connectés : utilisateurs qui ne se sont jamais connectés à votre instance.
- Utilisateurs non connectés depuis le mois dernier : utilisateurs qui ne se sont pas connectés au cours des 30 derniers jours.
- Utilisateurs non connectés depuis les 6 derniers mois : utilisateurs qui ne se sont pas connectés au cours des 6 derniers mois.
- Utilisateurs non connectés depuis 1 an : utilisateurs qui ne se sont pas connectés au cours de l'année écoulée.
- Besoin de réinitialiser le mot de passe : utilisateurs qui doivent réinitialiser leur mot de passe.
- Échecs de la réinitialisation du mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

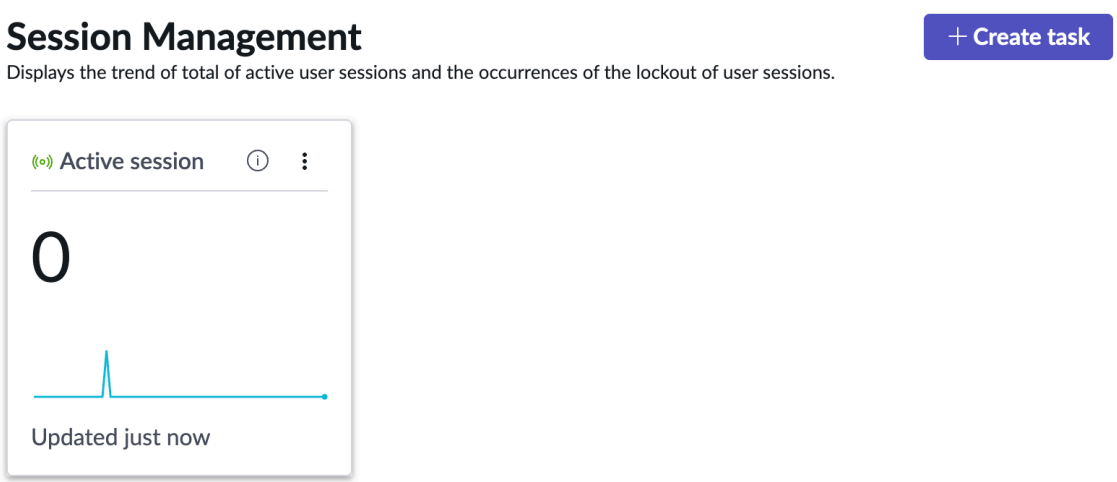
Sélectionnez les cartes pour afficher la page des mesures individuelles avec des détails supplémentaires.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

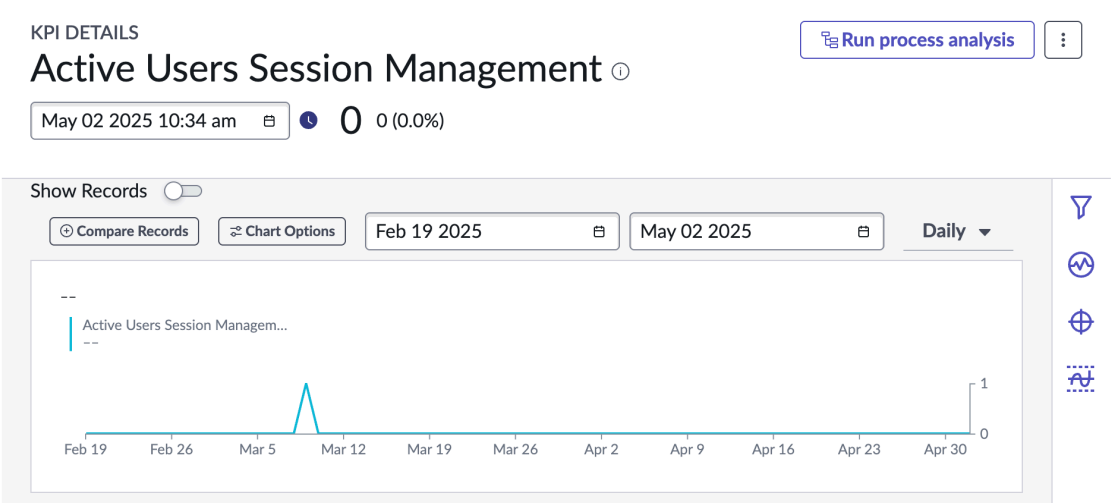
Gestion des sessions

Affichez les mesures relatives aux sessions utilisateur et la fréquence des verrouillages des sessions.

La page affiche une carte qui affiche une ligne de tendance des sessions actives, représentant le nombre de sessions actives sur votre instance.



Sélectionnez la carte pour afficher des détails supplémentaires.



À partir de la page de détails, vous pouvez utiliser les boutons situés sur le bord de l'écran pour configurer les filtres, les signaux KPI, les cibles et les seuils.

Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs

Affichez la ligne de tendance du nombre total d'utilisateurs (actifs et inactifs) et leur activité sur le ServiceNow AI Platform.

La section Vue d'ensemble des utilisateurs affiche la ligne de tendance du nombre total d'utilisateurs (actifs et inactifs) et leur activité sur le ServiceNow AI Platform.

Vous trouverez ci-dessous une explication du type d'utilisateurs :

- Total des utilisateurs : nombre total d'utilisateurs sur votre instance.
- Utilisateurs actifs : nombre total d'utilisateurs qui ont initié des sessions sur votre instance.
- Utilisateurs inactifs : utilisateurs qui ne se sont pas récemment connectés à votre instance.
- Utilisateurs inactifs qui ne sont pas bloqués : utilisateurs qui ne se sont pas récemment connectés mais qui ont toujours accès à leur compte.
- Nouveaux utilisateurs : utilisateurs qui ont récemment été ajoutés à votre instance.
- Connexions réussies : utilisateurs qui se sont connectés avec succès.
- Échecs de connexion : tentatives de connexion infructueuses.
- Connexions externes : authentifications qui utilisent une tierce partie.
- Connexions locales non protégées par MFA : connexions qui n'utilisent pas la MFA.
- Utilisateurs non connectés depuis le mois dernier : utilisateurs qui ne se sont pas connectés au cours des 30 derniers jours.
- Utilisateurs non connectés depuis les 6 derniers mois : utilisateurs qui ne se sont pas connectés au cours des 6 derniers mois.
- Utilisateurs non connectés depuis 1 an : utilisateurs qui ne se sont pas connectés au cours de l'année écoulée.
- Besoin de réinitialiser le mot de passe : utilisateurs qui doivent réinitialiser leur mot de passe.
- Échecs de la réinitialisation du mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Sélectionnez la carte pour afficher des détails supplémentaires.

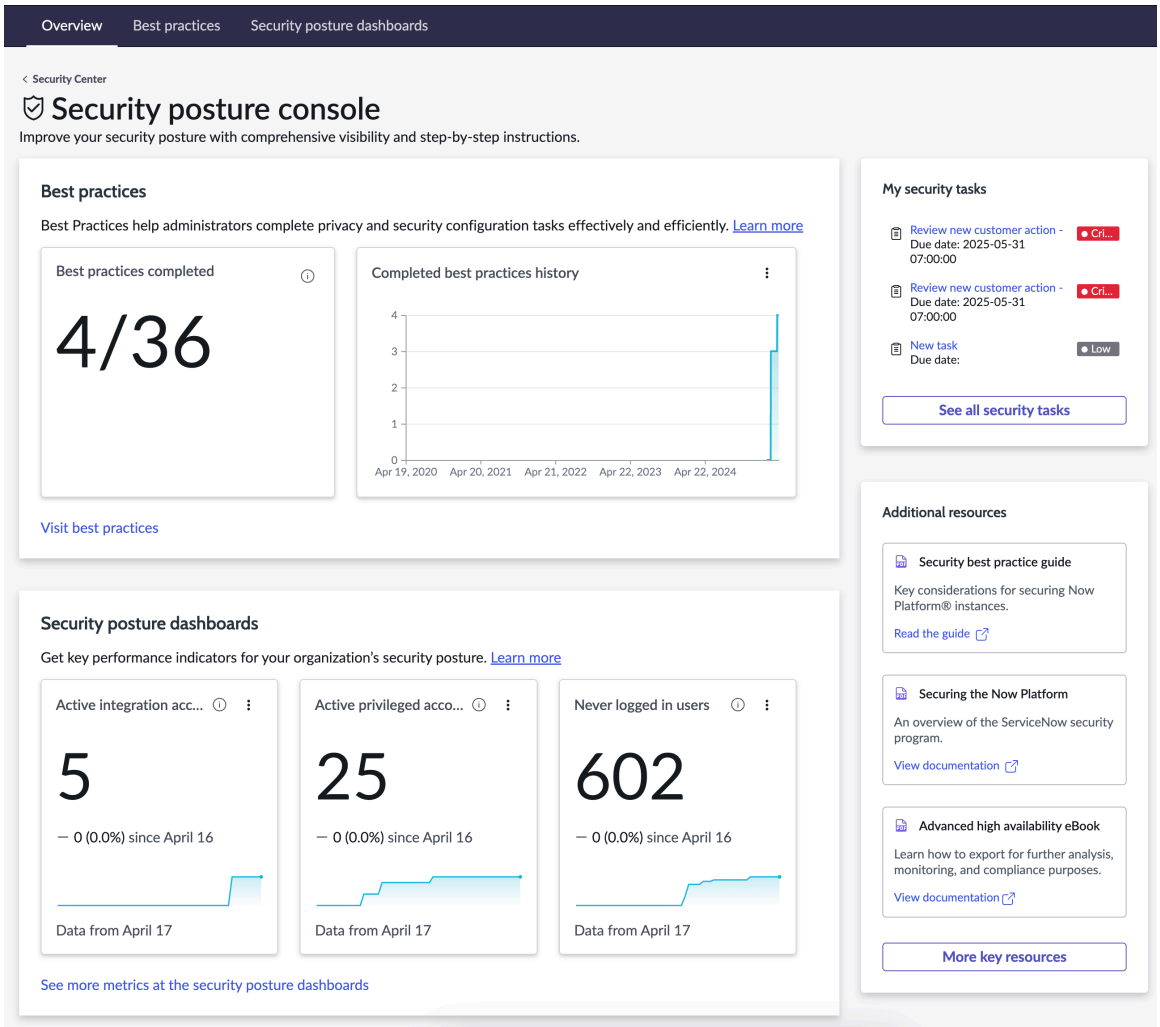
Sélectionnez le bouton **+Créer une tâche** pour créer une tâche de sécurité associée à une mesure. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Console de posture de sécurité

Améliorez votre capacité à identifier, à répondre aux menaces de sécurité et à vous en remettre grâce à une visibilité complète et à des instructions détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La console de posture de sécurité est divisée en sections pour fournir des informations sur les bonnes pratiques et les tableaux de bord de posture de sécurité. Trouvez des détails supplémentaires en sélectionnant l'une des cartes dans ces sections. Vous pouvez également utiliser la barre en haut de la page pour naviguer entre cette page et la section Bonnes pratiques et tableaux de bord de la posture de sécurité du Centre de sécurité.

Bonnes pratiques

Cette section affiche le nombre de bonnes pratiques et le nombre que vous avez appliquées à votre instance. Vous pouvez afficher un graphique montrant vos bonnes pratiques achevées au fil du temps.

Tableaux de bord sur la posture de sécurité

Cette section affiche le nombre de comptes d'intégration actifs, de comptes privilégiés actifs et d'utilisateurs qui ne se sont jamais connectés.

Comptes d'intégration actifs

Les comptes d'intégration sont des comptes d'utilisateurs qui gèrent les intégrations entre votre instance et des applications tierces.

Comptes privilégiés actifs

Les utilisateurs privilégiés sont des utilisateurs auxquels des rôles supplémentaires ont été affectés par des administrateurs pour accéder aux fonctionnalités telles que Paramètres de sécurité élevée, Importation et Utilisateurs du portail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs jamais connectés

Comptes d’utilisateurs qui ne se sont jamais connectés à votre instance.

Mes tâches de sécurité

Affichez les tâches de sécurité les plus urgentes qui vous sont affectées. Sélectionnez une tâche pour en afficher les détails, ou sélectionnez **Afficher toutes les tâches de sécurité** pour afficher une liste complète des tâches de sécurité.

Ressources supplémentaires

Utilisez la section Ressources supplémentaires située sur le bord de l’écran pour accéder à la documentation et aux vidéos relatives à l’apprentissage du Centre de sécurité, ainsi qu’à des informations sur la gestion de la sécurité de l’instance.

Bonnes pratiques de sécurité

Utilisez les bonnes pratiques de sécurité pour implémenter des tâches de configuration de la confidentialité et de la sécurité sur votre ServiceNow instance.

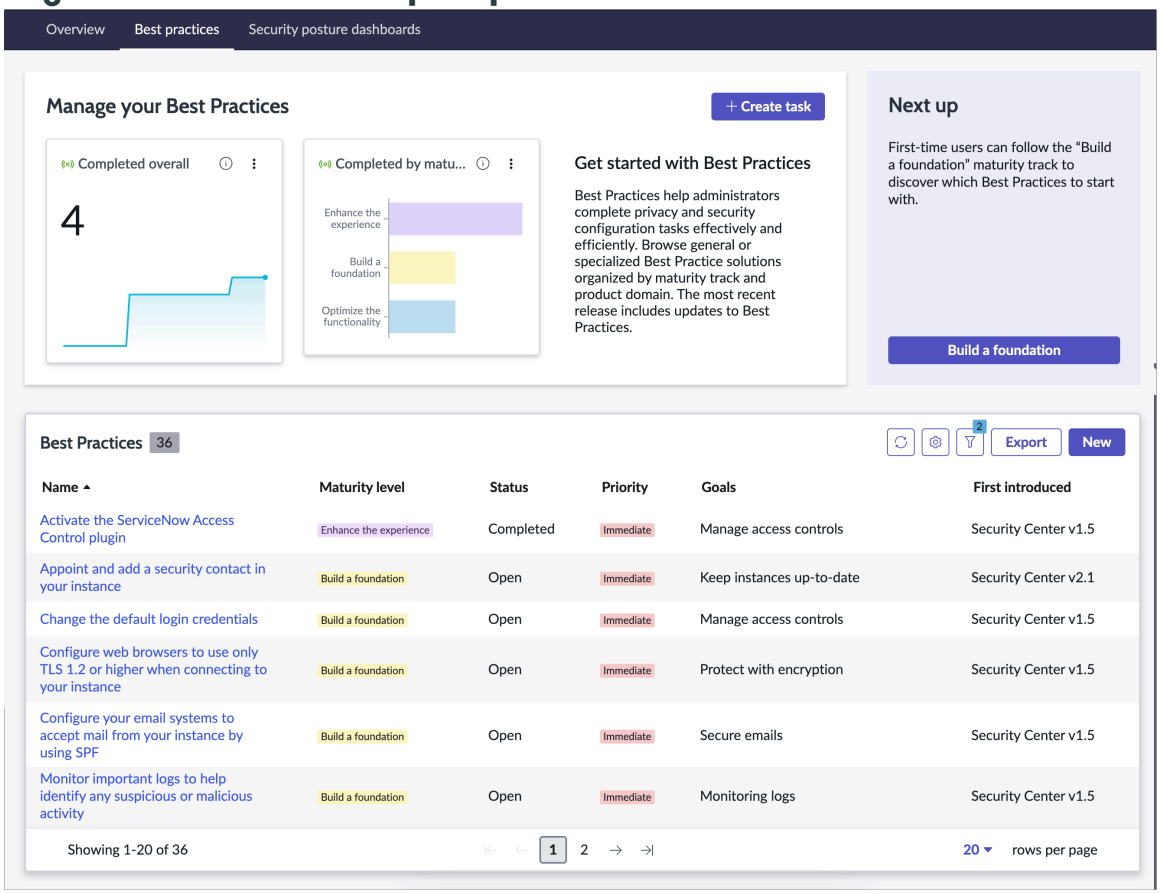
Identifiez les meilleures pratiques pour améliorer votre posture de sécurité et suivez les instructions étape par étape sur la façon de les implémenter. Les bonnes pratiques de sécurité fournissent les éléments suivants :

- La page d’accueil affiche une vue d’ensemble de vos progrès dans l’implémentation des bonnes pratiques de sécurité. Vous pouvez également organiser et gérer des listes de bonnes pratiques de sécurité en fonction des objectifs de votre organisation.
- La page de vue d’ensemble fournit des détails sur chaque bonne pratique de sécurité, les étapes pour les implémenter, ainsi qu’un enregistrement de toutes les activités et commentaires.
- La page Étapes de la tâche vous fournit des instructions sur la façon d’implémenter les bonnes pratiques de sécurité.
- La page Activité suit l’historique des actions de l’utilisateur et du système liées à vos bonnes pratiques de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil des bonnes pratiques de sécurité



La page d'accueil affiche une section **Gérer vos bonnes pratiques** , qui comprend des graphiques qui fournissent une vue d'ensemble de votre progression.

Globalement terminé

Affiche un nombre et une ligne de tendance des bonnes pratiques que vous avez complétées. Sélectionnez la carte pour afficher la page **Mesure globale terminée** dans Mesures de sécurité.

Terminé par niveau de maturité

Affiche un graphique des bonnes pratiques terminées, organisées par niveau de maturité (voir la description des niveaux de maturité dans le tableau précédent). Sélectionnez la carte pour afficher la page de mesure **Terminé par niveau de maturité** dans Mesures de sécurité.

Créer une base

Sélectionnez le bouton **Créer une base** pour filtrer la table de cette page afin d'afficher uniquement les bonnes pratiques dans le niveau de maturité Créer **une base** . Il s'agit de changements à faible impact que vous pouvez apporter pour commencer à améliorer la sécurité de l'instance.

Créer une tâche

Utilisez le bouton **+Créer une tâche** pour créer une tâche de sécurité et suivre ou déléguer le travail de bonnes pratiques. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

La table vous permet d'appliquer des filtres afin de trier et d'enregistrer des listes filtrées, que vous pouvez utiliser comme listes de travail pour différents cas d'utilisation ou rôles. Consultez Enregistrer une liste filtrée pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous trouverez ci-dessous des explications sur les champs associés à la table des bonnes pratiques de sécurité.

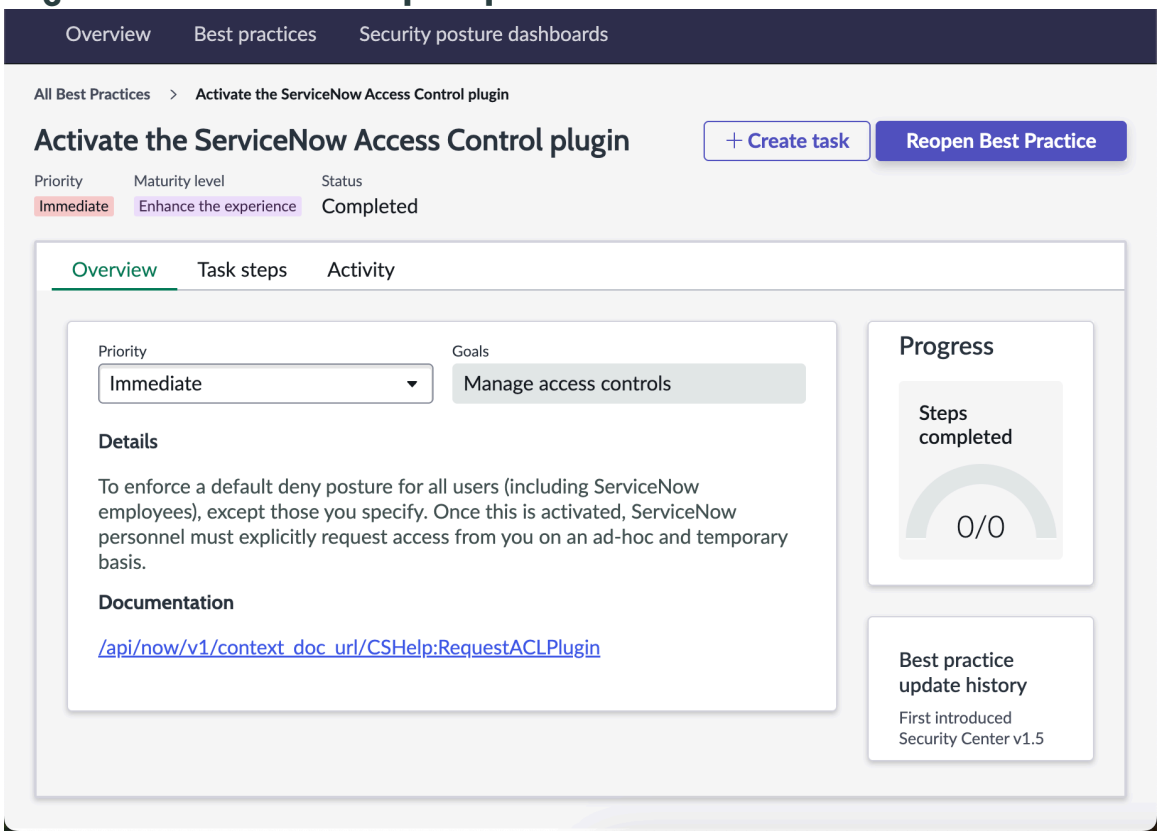
Résumé des champs utilisés dans la table des bonnes pratiques de sécurité

Nom	Description
Nom	Mot utilisé pour identifier une bonne pratique de sécurité.
Niveau de maturité	Applications et fonctionnalités qui ont été classées par ordre d'impact pour vous fournir des résultats mesurables. Les valeurs des niveaux de maturité sont les suivantes : • Créer une base • Améliorer l'expérience • Optimiser la fonctionnalité • Ajouter des fonctionnalités avancées Ceux-ci peuvent également être considérés comme des phases ramper, marcher, courir et voler.
Statut	État actuel d'une bonne pratique : • Ouvert • En cours • Terminé
Priorité	Ordre d'importance pour l'implémentation d'une bonne pratique dans votre organisation : • Immédiat • Plus tard • Non applicable
Objectifs	Catégorie de sécurité qu'une bonne pratique traite : • Résoudre les configurations de sécurité initiales • Sécuriser les e-mails • Journaux de surveillance • Gérer les contrôles d'accès • Protéger avec chiffrement • Maintenir les instances à jour
Date de première introduction	Version de Security Center à laquelle la bonne pratique a été introduite.
Modifié	Version de Security Center à laquelle la bonne pratique a été changée.
Supprimé	Version de Security Center à laquelle la bonne pratique a été supprimée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page détaillée des bonnes pratiques de sécurité



Sélectionnez une bonne pratique dans la table pour afficher sa page. En haut de la page de détails, vous pouvez afficher des informations générales sur les bonnes pratiques de sécurité, notamment la priorité, le niveau de maturité et l'état. Utilisez le bouton **Terminer les bonnes pratiques** pour marquer une pratique comme terminée ou le bouton **Rouvrir les bonnes pratiques** pour marquer la pratique comme terminée. Utilisez le **bouton +Créer une tâche** pour créer une tâche de sécurité qui permet de suivre et de déléguer cette tâche. Pour en savoir plus sur les tâches de sécurité, reportez-vous à la section Tâches de sécurité.

Cette page fournit plus d'informations sur les bonnes pratiques, divisées en onglets :

Vue d'ensemble

Cet onglet contient le menu déroulant **Priorité** , qui vous permet de spécifier les bonnes pratiques de sécurité qui sont importantes pour vous à ce moment-là et qui ne sont pas applicables.

La section Détails fournit du contenu sur les fonctionnalités associées aux bonnes pratiques de sécurité et la section Documentation fournit un ou plusieurs liens où vous pouvez trouver des informations supplémentaires.

La carte **de progression** sur la droite indique le nombre d'étapes terminées par rapport au nombre total d'étapes incluses. Sélectionnez **Accéder à l'étape suivante** pour accéder à l'étape incomplète suivante.

La carte **d'historique de mise à jour des bonnes pratiques** fournit un instantané des informations de la version pour la bonne pratique. Vous pouvez suivre la version de ServiceNow Security Center dans laquelle la bonne pratique de sécurité a été publiée et les versions dans lesquelles elle a ensuite été mise à jour pour la dernière fois.

Étapes de la tâche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet onglet fournit des instructions étape par étape sur la façon d'implémenter cette bonne pratique de sécurité. Pour plus d'informations, consultez Terminer une bonne pratique de sécurité .

Activité

Ce tableau affiche les activités horodatées répertoriées de la plus récente à la plus ancienne. Utilisez la recherche et le filtre pour obtenir des informations. Pour plus d'informations, consultez Appliquer des filtres à la table des bonnes pratiques de sécurité .

Suivre une bonne pratique de sécurité

Découvrez comment mettre en œuvre une bonne pratique de sécurité sur votre instance ServiceNow.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Effectuez les étapes suivantes pour implémenter les bonnes pratiques de sécurité sur votre instance ServiceNow.

Procédure

1. Accédez aux bonnes pratiques de sécurité en sélectionnant **Tout** sur votre instance ServiceNow, puis en saisissant **les bonnes pratiques**.
2. Appliquez un filtre pour afficher les bonnes pratiques de sécurité à implémenter.
   a. Accédez à la table **Bonnes pratiques** dans l'interface utilisateur.
   b. Sélectionnez le menu kebab ou l'élément avec trois points ⋮) dans la colonne **État** .
   c. Sélectionnez les options **Ouvert** et **En cours** , puis sélectionnez **Appliquer**.
3. Sélectionnez le nom d'une bonne pratique de sécurité à implémenter.
4. Sélectionnez **Passer à l'étape suivante**.
5. Sélectionnez une étape de tâche dans la liste des **étapes** de la tâche.
6. Sélectionnez l'icône du chevron vers le bas (v) pour afficher les instructions d'implémentation de cette étape.
7. Lisez les instructions, puis implémentez-les sur votre instance ServiceNow.
8. Sélectionnez **Marquer l'étape comme terminée** lorsque vous avez terminé la tâche.

> **Remarque :**
> Vous pouvez ignorer la tâche si vous souhaitez y revenir ultérieurement ou si elle ne s'applique pas aux objectifs de votre organisation. En outre, vous pouvez rouvrir une étape de tâche terminée en sélectionnant l'étape de tâche, puis **l'étape Redémarrer**.

9. Sélectionnez **Bonne pratique complète**.

Vous pouvez suivre une bonne pratique de sécurité à tout moment. Vous n'êtes pas obligé de terminer toutes les étapes et ce n'est pas grave si vous les sautez. Toutefois, envisagez d'insérer un commentaire dans le sous-onglet Activité lors de l'exécution d'une bonne pratique de sécurité lorsque vous n'avez pas terminé toutes les étapes pour une référence d'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher l'activité d'une bonne pratique

Suivez l'historique chronologique et horodaté d'une bonne pratique de sécurité que vous effectuez sur votre instance ServiceNow, ainsi que l'utilisateur à l'origine de l'activité.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez au gestionnaire des bonnes pratiques de sécurité en sélectionnant **Tout** sur votre instance ServiceNow, puis saisissez Bonnes pratiques.
2. Dans la table Bonnes pratiques, sélectionnez une bonne pratique de sécurité pour laquelle vous souhaitez afficher l'activité dans la colonne **Nom** .
3. Sélectionnez l'onglet **Activité** .

Parmi les exemples d'activités que vous pouvez afficher, citons les changements de champs, par exemple si l'état d'une bonne pratique de sécurité est passé d'Ouvert à Terminé, ou lorsqu'une étape de tâche est terminée ou ignorée. En outre, vous pouvez saisir des informations supplémentaires relatives à une activité en saisissant un commentaire dans la zone de texte.

Afficher les données des bonnes pratiques achevées

Consultez des représentations visuelles du nombre total de bonnes pratiques achevées ou segmentées par niveau de maturité.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Terminez les actions pour afficher les graphiques qui fournissent des tendances visuelles des bonnes pratiques de sécurité qui ont été complétées dans l'ensemble et par niveau de maturité.

Procédure

1. Accédez à l'application Centre de sécurité et accédez à l'onglet **Bonnes pratiques** .
2. Sous la carte **Gérer vos bonnes pratiques** , sélectionnez le graphique **global Terminé** .
3. Consultez le graphique pour afficher les tendances relatives aux configurations des bonnes pratiques de sécurité qui ont été effectuées.
4. Sélectionnez **Terminé par niveau de maturité** pour afficher un graphique affichant les tendances des bonnes pratiques appliquées par niveau de maturité.

Filtre la table des bonnes pratiques de sécurité

Appliquez des filtres pour renvoyer des résultats plus pertinents pour vos bonnes pratiques de sécurité.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez au gestionnaire des bonnes pratiques de sécurité en sélectionnant **Tout** sur votre instance ServiceNow et en saisissant la bonne pratique.
2. Accédez à la table **Bonnes pratiques** et sélectionnez un champ auquel vous souhaitez appliquer un filtre en sélectionnant son menu de kebab ou celui avec trois points ⋮).

Enregistrer un filtre pour une utilisation ultérieure

Découvrez les étapes d'enregistrement des filtres dans vos bonnes pratiques de sécurité pour une réutilisation ultérieure.

Avant de commencer

Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Après avoir créé des filtres dans la table des bonnes pratiques de sécurité, vous pouvez les enregistrer pour les utiliser lors de votre prochaine authentification dans votre instance. Si vous souhaitez plus de flexibilité sur le type de filtres que vous pouvez créer, vous pouvez appliquer un filtre avancé.

Procédure

1. Sélectionnez l'icône du panneau Afficher le filtre (icône de ⏷).
2. Dans le panneau de dialogue **Filtre** , faites défiler vers le bas et sélectionnez **Vue avancée**.
3. Créez un filtre en ajoutant des conditions qui contiennent un champ, un opérateur et des valeurs.
4. Sélectionner **Enregistrer le filtre**
5. Entrez le nom du filtre.
6. Sélectionnez une autorisation.
7. Sélectionnez **Enregistrer**.
8. Sélectionnez **Mettre à jour** pour appliquer le filtre enregistré à la table des bonnes pratiques de sécurité.

Utiliser un filtre enregistré

Découvrez les étapes d'utilisation des filtres que vous avez enregistrés pour vos bonnes pratiques de sécurité.

Avant de commencer

Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Une fois que vous vous êtes déconnecté de votre instance, vos filtres sont réinitialisés aux paramètres par défaut. Les étapes suivantes montrent comment récupérer un filtre enregistré afin de pouvoir le réappliquer sur la table des bonnes pratiques de sécurité.

Procédure

1. Sélectionnez l'icône Afficher le panneau de filtre (icône de ⏷).
2. Dans la boîte de dialogue Filtre, faites défiler vers le bas et sélectionnez **Vue avancée**.
3. Sélectionnez **Utiliser le filtre existant**, puis sélectionnez un filtre enregistré dans la liste déroulante.
4. Sélectionnez **Mettre à jour** pour appliquer le filtre enregistré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonnes pratiques

Découvrez les détails des bonnes pratiques dans la console de posture de sécurité.

Bonne pratique	Description
Activer le module d'extension de contrôle d'accès ServiceNow	Utilisez le module d'extension Contrôle d'accès ServiceNow pour contrôler quels employés peuvent accéder à votre instance et quand. Application d'une posture de refus par défaut pour tous les utilisateurs, à l'exception des utilisateurs que vous spécifiez. Cela peut inclure les ServiceNow employés. L'utilisation de ce module d'extension empêche tout accès indésirable à votre instance. **Remarque :** Une fois ServiceNow le contrôle d'accès activé, le personnel doit explicitement demander l'accès sur une base ad hoc et temporaire. Pour en savoir plus sur ce module d'extension, reportez-vous à la section Contrôle d'accès ServiceNow.
Nommer et ajouter un contact de sécurité dans votre instance	Sélectionnez un contact pour la sécurité des informations au sein de votre organisation qui reçoit des informations relatives à la sécurité de la part de l'équipe de sécurité. Ce contact s'ajoute à votre administrateur, qui reçoit également ces mises à jour. Il peut s'agir de problèmes de sécurité, d'alertes de sécurité ou de détails sur des mises à jour logicielles importantes. Pour plus de détails sur l'ajout d'un contact de sécurité, consultez KB0621516.
Changer les informations d'identification de connexion par défaut	Modifiez les mots de passe des comptes utilisateur intégrés de votre instance, tels que administrateur, ITIL et employé. Ces comptes sont approvisionnés avec des mots de passe par défaut, propres à votre instance, mais doivent être modifiés dès que possible. Pour en savoir plus sur la modification des mots de passe des comptes d'utilisateurs sur votre instance, reportez-vous à la section Configurer le mot de passe d'un utilisateur.
Configurer les navigateurs Web pour utiliser uniquement TLS 1.2 ou une version ultérieure lors de la connexion à votre instance	Vérifiez que les navigateurs qui se connectent à votre instance utilisent le protocole TLS (Transport Layer Security) 1.2, plus sécurisé. Cette modification peut être effectuée sur le navigateur ou appliquée par votre proxy web ou une autre passerelle. Consultez la documentation de votre navigateur, proxy web ou passerelle pour connaître les étapes de configuration de ces produits afin qu'ils utilisent uniquement TLS 1.2.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
Configurez vos systèmes de messagerie pour qu'ils acceptent les e-mails de votre instance à l'aide de SPF	Si votre organisation utilise le Cadre de travail des politiques de l'expéditeur (SPF) pour contrôler les e-mails entrants à l'aide de la technologie anti-spam, vous devez la configurer pour accepter les e-mails provenant de votre instance. Configurez SPF pour interroger les enregistrements SPF de manière dynamique. Si SPF n'est pas une option, une autre approche consiste à ajouter les adresses IP du serveur de messagerie à votre liste d'autorisation. Cette configuration doit être surveillée car les adresses peuvent être sujettes à changement. Pour connaître les étapes et en savoir plus sur ces solutions, reportez-vous à la rubrique KB0535456
Envisagez de limiter les pièces jointes, les chargements et les téléchargements de fichiers	Limitez les chargements de pièces jointes par rôle, extension de fichier, type MIME ou taille afin d'éviter le stockage et la livraison de fichiers potentiellement malveillants à partir de votre instance. Vous pouvez également contrôler les types de fichiers qui peuvent être téléchargés, y compris par type MIME, et empêcher l'accès aux images par les utilisateurs non authentifiés. Ces restrictions de pièce jointe sont contrôlées par les propriétés système de votre instance. Pour plus d'informations sur leur configuration, reportez-vous à la section Configure attachment system properties .
Désactiver les messages SQL du navigateur	Empêchez les messages d'erreur SQL d'être présentés dans le navigateur Web. Bien qu'utiles aux utilisateurs et aux développeurs, ces messages peuvent être utilisés par les attaquants pour obtenir des informations sur votre système ou pour guider leurs tentatives d'accès à vos données. Ces messages peuvent être désactivés à l'aide d'une propriété système. Pour en savoir plus sur cette propriété système, reportez-vous à la section Désactiver les messages d'erreur SQL [Mis à jour dans Centre de sécurité 1.3 et 1.5].
Désactiver l'authentification sans mot de passe	Garantissez une authentification forte en désactivant l'authentification sans mot de passe lorsque cela est possible. Sans désactiver l'authentification sans mot de passe, les attaquants potentiels pourraient accéder à votre instance en devinant correctement un nom d'utilisateur (tel que prenom.nom ou titre de rôle). Vous pouvez désactiver l'authentification sans mot de passe sur votre instance à l'aide d'une propriété système. Pour obtenir des détails sur cette propriété, consultez Désactiver l'authentification sans mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
Activer l'audit de table pour les données importantes ou sensibles	Suivez les changements apportés à vos données à l'aide de l'audit de table. L'audit suit la création, la mise à jour et la suppression de tous les enregistrements dans la table où il est activé, ce qui permet aux administrateurs de suivre les changements apportés aux données importantes ou sensibles. Les administrateurs peuvent également choisir de sélectionner des champs spécifiques dans une table pour l'audit afin d'afficher des résultats plus ciblés ou de réduire l'impact sur les performances. Pour plus d'informations sur l'audit des instances, reportez-vous à la section Audit. Pour obtenir des instructions spécifiques sur l'activation de l'audit sur une table, reportez-vous à la section Configuration de l'audit pour une table.
Chiffrer les données au repos au sein de l'instance	Chiffrez vos données pour préserver leur confidentialité et leur intégrité. Les données de votre instance peuvent se trouver dans la base de données. Vous pouvez également choisir de vous abonner à une fonctionnalité permettant de chiffrer le volume de données de manière transparente sur le backend. Les disques physiques sur lesquels l'instance s'exécute peuvent également être entièrement chiffrés pour protéger les données en cas de perte ou de vol. Vous pouvez utiliser différentes méthodes de chiffrement simultanément pour les données stockées dans votre instance, en fonction de votre cas d'utilisation et des risques que vous souhaitez atténuer. Par exemple, vous pouvez choisir de chiffrer de manière transparente vos données au repos à l'aide du chiffrement de la base de données sur la plupart des tables, du chiffrement dans le cloud sur l'ensemble du volume de données. Vous pouvez également utiliser le chiffrement matériel complet du disque, qui nécessite également un environnement dédié pour se protéger contre le vol de disque ou de serveur. Examinez les options de chiffrement disponibles dans .Key Management Framework
Imposer l'utilisation de phrases de passe fortes	Utilisez des politiques de mot de passe pour appliquer la longueur, la complexité, l'expiration, l'unicité, le verrouillage et plus encore pour les comptes natifs et locaux sur votre instance. Utilisez ces stratégies pour maximiser la sécurité, encourager l'adoption de phrases de sécurité longues et éliminer l'utilisation de mots de passe simples. Vous pouvez conserver vos politiques existantes pour tous les services d'authentification externes que vous avez intégrés, tels que LDAP ou SAML.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	Pour en savoir plus sur la configuration de la stratégie de mot de passe, reportez-vous à la section Configurez votre politique de mot de passe.
Garantir la création automatique de compte	Utilisez cette fonctionnalité pour créer dynamiquement des comptes d'utilisateurs par e-mail. N'activez cette fonctionnalité que si elle est nécessaire pour vos besoins professionnels, uniquement après avoir défini une liste de domaines de confiance à partir desquels des comptes peuvent être créés. Vous pouvez également contrôler la manière dont les mots de passe sont attribués aux nouveaux comptes créés de cette façon. Pour plus d'informations sur la création automatique d'utilisateurs, reportez-vous à la section Enable automatic user creation .
Garantir un accès sécurisé aux bases de connaissances	Gérez l'accès aux bases de connaissances et aux articles pour garantir un partage sécurisé et efficace des informations. Vous pouvez déterminer si certains utilisateurs ou catégories d'utilisateurs peuvent accéder aux bases de connaissances et aux articles de la base de connaissances en contrôlant l'accès en contribution et en lecture. La configuration spécifique dépend des besoins de votre entreprise. Pour en savoir plus sur les options de configuration de l'accès aux connaissances, consultez Managing access to knowledge bases and knowledge articles .
Assurez-vous que le module d'extension de haute sécurité est installé et activé	Utilisez le module d'extension de haute sécurité (HSP) pour améliorer la gestion de la sécurité et appliquer les paramètres appropriés. Les paramètres de sécurité élevée fournissent un emplacement central pour les paramètres de sécurité, créent un rôle d'administrateur de sécurité distinct, une propriété de refus par défaut et d'autres fonctionnalités de sécurité importantes. HSP est installé et activé par défaut sur toutes les nouvelles instances. Vous pouvez demander l'activation HSP pour les instances plus anciennes, y compris les instances qui ont fait l'objet de mises à niveau à partir d'une version antérieure. L'activation de HSP ne doit être effectuée qu'après des tests minutieux dans un environnement de non-production, car l'activation modifie certaines propriétés et comportements fondamentaux. Pour en savoir plus sur le module d'extension Sécurité élevée, reportez-vous à la section Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
Familiarisez-vous avec les ressources de sécurité NOW	Les informations de sécurité évoluent constamment, il est donc crucial de rester à jour avec les ressources de sécurité pour maintenir la sécurité de vos informations. Utilisez les ressources suivantes pour rester informé sur les ressources de sécurité : • Répertoire CORE : Portail de conformité ServiceNow CORE • Sécurisation de la plateforme d'IA ServiceNow : comment ServiceNow protège les données des clients • Sécuriser votre instance
Renforcer votre instance	Utilisez l'outil de sécurisation renforcée du centre de sécurité pour réduire les risques en limitant les faiblesses qui pourraient être exploitées, et implémentez les paramètres recommandés pour sécuriser davantage votre instance. Pour en savoir plus sur le Centre de sécurité, consultez Centre de sécurité. Passez en revue les paramètres de sécurisation renforcée disponibles à l'adresse Paramètres de sécurisation renforcée.
Installez les correctifs dès que possible	Installez les correctifs et les mises à jour de plateforme dès que possible pour garantir les niveaux de sécurité les plus élevés pour votre instance et celles des autres clients. Rester à jour avec les mises à jour vous permet également de maintenir un support continu en vous conformant à la politique de fin de vie. Utilisez le Centre de mise à niveau pour faciliter la gestion du processus. Des correctifs de sécurité sont régulièrement publiés pour la Now Platform via les correctifs et les correctifs d'urgence qui accompagnent les mises à jour des fonctionnalités du produit. La mise à niveau lorsque de nouveaux correctifs sont disponibles permet de réduire le risque de vulnérabilités potentielles. Vous trouverez des informations sur les versions, les correctifs et les correctifs d'urgence de la Now Platform dans la section Notes de version de la documentation du produit. Pour plus d'informations, consultez Phase 1 - .
Intégration MFA	Intégrez l'authentification multifacteur (MFA) tierce à votre IdP SAML existant pour fournir une sécurité de connexion supplémentaire. La MFA offre un niveau de sécurité élevé, car l'authentification nécessite plusieurs facteurs d'authentification. Quelque chose que l'utilisateur connaît (le mot de passe) ainsi que quelque chose qu'il

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	possède (un code à usage unique, un téléphone portable ou des attributs biométriques, tels qu'une empreinte digitale). Pour en savoir plus sur l'intégration MFA, consultez Authentification multifacteur.
Limiter les domaines d'expéditeur d'e-mail acceptés	Contrôlez les domaines et les utilisateurs avec lesquels votre instance peut communiquer par e-mail à l'aide des filtres d'adresse système. Ces filtres peuvent être personnalisés en fonction de vos besoins. Découvrez comment configurer les domaines de confiance dans Désigner des domaines d'e-mail comme n'étant pas de confiance ou n'étant pas de confiance.
Surveillez les journaux importants pour identifier toute activité suspecte ou malveillante	Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance. **Journaux des événements** Les journaux des événements révèlent beaucoup d'informations sur l'activité du système, y compris les événements de connexion (réussie ou non) et l'escalade des privilèges. **Journaux système** Les journaux système contiennent des informations détaillées sur l'activité générale, y compris les changements de configuration, les erreurs système, les workflows et les connexions de données entrantes/sortantes. **Remarque :** Les journaux des événements et du système peuvent également être utilisés pour fournir une piste d'audit de toute activité du personnel. **Journaux de transactions** Les journaux des transactions enregistrent toutes les activités liées au navigateur Web pour une instance et peuvent fournir des détails sur chaque demande effectuée. Les journaux des transactions peuvent être utiles pour identifier les activités inhabituelles ou malveillantes. **Audit des tables et historique des enregistrements** Activez l'audit pour les tables de base de données. L'historique des enregistrements est perpétuel et vous permet de suivre et d'afficher les détails de toutes les modifications apportées aux données depuis leur création. Par défaut, seules les tables d'incidents, de problèmes et de changements sont suivies. Pour les autres tables, l'audit doit être activé manuellement. **Journaux d'importation**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	Vous pouvez afficher des informations détaillées relatives à l'activité d'importation de données dans votre instance en consultant les journaux d'importation. Ces journaux incluent des informations sur la source et le statut, l'heure, etc **Journaux des services Web sortants** Ceux-ci montrent l'activité des demandes REST et SOAP et peuvent vous aider à suivre le volume et la destination des connexions à des services externes. En savoir plus sur les connexions système dans Journaux système.
Surveiller les taux d'échec de connexion et créer des alertes	Surveillez les activités inhabituelles telles qu'un nombre élevé d'échecs de connexion, en particulier dans des délais courts. Vous pouvez créer des alertes pour envoyer des e-mails lorsqu'un seuil que vous définissez est dépassé. Découvrez comment configurer ces seuils dans .Indicator thresholds
Surveiller les événements de sécurité	Passez en revue le **tableau de bord Mes mesures de sécurité** pour voir les mesures de sécurité disponibles pour votre instance et définir des seuils pour générer des notifications par e-mail en cas d'activité notable. Voici quelques exemples d'activités notables : **Escalade de privilège** Des modifications inattendues apportées aux rôles privilégiés, tels que Administrateur, ITIL_Admin ou tout autre rôle disposant de privilèges plus élevés, peuvent indiquer des actions suspectes. **Échecs de connexion** Un nombre inhabituel ou des schémas inhabituels d'échecs de connexion peuvent révéler des tentatives potentielles par force brute ou des attaques par pulvérisation de mot de passe. **Administrateurs et utilisateurs à privilèges élevés ajoutés** La validité de la création d'un nouveau compte administrateur doit être vérifiée afin d'empêcher les tentatives d'accès privilégié non autorisé.
Surveiller le niveau de conformité à la sécurisation renforcée de votre instance	Assurez-vous que vos instances sont en conformité avec les dernières mesures de sécurisation renforcée de sécurité à l'aide de l'outil de sécurisation renforcée du Centre de sécurité. Accéder à cet outil dans une instance de non-production Évaluez l'impact sur votre environnement. Idéalement, le score doit être aussi proche que possible de 100 % avec un score minimum de 83 %, sans affecter les fonctionnalités du produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	Pour en savoir plus sur l'outil de paramètres de sécurisation renforcée du Centre de sécurité, consultez Paramètres de sécurisation renforcée.
Renvoyez vos développeurs au Guide de codage sécurisé	Assurez-vous que votre instance est sécurisée et résistante autant que possible aux accès non autorisés à l'aide de pratiques de codage sécurisées. Le guide de codage sécurisé ServiceNow pour les développeurs d'instances fournit une vue d'ensemble des classes et méthodes GlideScriptable liées à la sécurité des applications proposées par ServiceNow. Ce guide est conçu pour aider et éduquer les développeurs lors de la création et de la modification du code sur l'instance cible. Consultez le guide du Guide de codage sécurisé ServiceNow pour les développeurs d'instance .
Décochez la case « Se souvenir de moi »	Empêchez tout accès indésirable à votre instance en désactivant la fonctionnalité **Se souvenir de moi** . Lorsqu'elle est active, cette fonctionnalité stocke un cookie sur l'ordinateur de l'utilisateur, qui authentifie automatiquement l'utilisateur lors des visites suivantes. Cela peut poser des problèmes de sécurité si les utilisateurs accèdent à votre instance à partir d'un point de terminaison non sécurisé, tel qu'un ordinateur partagé. Pour en savoir plus sur cette fonctionnalité et sur la façon de la désactiver, consultez Mémoriser mon nom.
Restreindre l'accès à votre instance à partir d'adresses IP inconnues	Empêchez tout accès non autorisé à votre instance en restreignant l'accès à partir d'adresses IP non liées à votre organisation. Toute personne tentant d'accéder à l'instance à partir d'une adresse IP non autorisée est refusée. Si vous utilisez cette approche, envisagez d'autoriser uniquement les adresses externes de votre passerelle ou de votre proxy web, ainsi que les adresses à partir desquelles vos utilisateurs accèdent à l'instance, y compris les utilisateurs distants. Vous pouvez restreindre l'accès sortant et entrant par adresse IP. Découvrez comment restreindre l'accès à votre instance par adresse IP dans Restreindre l'accès aux module d'extension de plages d'adresses IP spécifiques [Mis à jour dans Centre de sécurité 1.3].
Consulter les conseils de sur ServiceNow les attaques par pulvérisation de mots de passe	Protégez votre instance contre les attaques par pulvérisation de mot de passe. Ces attaques tentent d'obtenir un accès en testant successivement un mot de passe couramment utilisé sur plusieurs comptes. Pour en savoir plus sur les attaques par pulvérisation et sur la manière d'en protéger vos instances, consultez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	Stratégies d’atténuation des attaques par pulvérisation de mot de passe .
Passer en revue le modèle de sécurité partagée	Comprenez votre rôle partagé en tant que client dans le maintien de la sécurité de vos instances en examinant le modèle de responsabilité partagée. Le modèle de responsabilité partagée définit le partenariat entre le client et le client, tous deux ayant des responsabilités spécifiques. Pour en savoir plus , consultez Modèle de responsabilité partagée ServiceNow .
Transférer les données de journal à partir de l'instance à des fins d'archivage et de référence	Archivez vos données de journal pour les conserver au-delà de la période de rotation de journaux de 21 jours par défaut. Cet archivage peut être réalisé à l’aide de demandes de services Web, de la fonction d’exportation de données, du serveur MID ou du service d’exportation de journaux à partir du package Vault. Utilisez les ressources suivantes pour en savoir plus sur ces méthodes : • Web services • Exploration Service d'exportation de journal (LES)
Utiliser des modules de chiffrement avec RBAC pour améliorer davantage le contrôle d'accès aux données	Découvrez comment utiliser le cadre de travail de gestion des clés (KMF) pour protéger les données de votre instance à l’aide du contrôle d’accès basé sur les rôles (RBAC). KMF utilise des modules de chiffrement qui vous permettent de définir quelles données de votre instance sont chiffrées et quelle méthode de chiffrement utiliser. L’utilisation de plusieurs modules vous permet de chiffrer différentes zones de votre instance avec différentes spécifications. Découvrez comment KMF et ses composants sont utilisés pour chiffrer vos données sur Explorer le cadre de gestion des clés. Pour en savoir plus sur les modules cryptographiques dans Vue d’ensemble du module de chiffrement.
Utilisation de l'authentification basée sur certificat avec les fournisseurs d'intégration	Configurez le trafic vers vos fournisseurs d’intégration à l’aide de connexions REST/SOAP pour utiliser l’authentification basée sur certificat. L’authentification par certificat SSL (Secure Socket Layer) chiffre les données en transit, ce qui permet d’éviter qu’elles ne soient lues lors de leur envoi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	Pour en savoir plus sur cette configuration, reportez-vous à la section Configurer l'authentification réciproque.
Utiliser l'authentification SAML	Intégrez l'authentification multifacteur (MFA) tierce à votre IdP SAML existant pour fournir une sécurité de connexion supplémentaire. La MFA offre un niveau de sécurité élevé, car l'authentification nécessite plusieurs facteurs d'authentification. Quelque chose que l'utilisateur connaît (le mot de passe) ainsi que quelque chose qu'il possède (un code à usage unique produit par un jeton MFA ou un téléphone portable, ou des attributs biométriques, tels qu'une empreinte digitale). ServiceNow prend en charge l'intégration MFA directe avec les comptes locaux, LDAP, SSO avec SAML, OIDC ou synthèse. L'authentification adaptative est un prérequis pour la SSO avec MFA. La MFA peut être activée pour des utilisateurs et des rôles spécifiés, et configurée pour faciliter l'utilisation. Par exemple, vous pouvez exempter les appareils reconnus pendant un certain nombre d'heures. Vous pouvez afficher les mesures pour l'utilisation de la MFA dans le Centre de sécurité. Apprenez-en plus sur l'authentification SAML à l'aide de ces ressources : • Concepts SAML 2.0 • Configuration SAML 2.0 à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs
Utiliser l'ensemble de fonctionnalités de filtres d'e-mail pour traiter les messages entrants suspects	Créez des filtres d'e-mail pour filtrer les messages marqués comme suspects par ServiceNow la protection antivirus. En plus de la protection antivirus, la protection antivirus analyse les e-mails à la recherche de logiciels malveillants et de spam, la notation et les résultats en ajoutant ces informations au message dans les en-têtes X. Vous pouvez utiliser ces en-têtes comme critères pour que le module d'extension Filtres d'e-mail agisse si vous le souhaitez. Pour en savoir plus sur ServiceNow la fonction antivirus de , consultez Analyse antivirus. Découvrez comment configurer les filtres d'e-mail sur votre instance dans Email filters .
Utiliser la sonde Syslog pour envoyer des journaux à votre SIEM	Utilisez la sonde syslog pour envoyer des ServiceNow messages de journal de votre instance à un gestionnaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bonne pratique	Description
	d'informations et d'événements de sécurité (SIEM). Un SIEM est un logiciel ou un service tiers qui peut être utilisé pour la surveillance des activités et l'identification des événements de sécurité. Pour en savoir plus sur la ServiceNow configuration de la sonde syslog, reportez-vous à la section Syslog probe .
Utilisez votre propre environnement de sécurité de messagerie mature	Envisagez d'utiliser votre propre infrastructure (ou celle d'un tiers) pour envoyer et recevoir des e-mails liés à l'instance et bénéficiez d'un contrôle plus précis du périmètre des e-mails. En utilisant vos propres serveurs SMTP, POP3 ou IMAP, vous pouvez contrôler la façon dont les messages sont filtrés et reçus avant d'être envoyés à votre instance. **Remarque :** La configuration de votre propre infrastructure de messagerie est considérée comme une configuration de messagerie avancée et peut éventuellement utiliser une infrastructure de messagerie tierce via l'authentification de messagerie OAuth 2.0. Pour plus d'informations, consultez la documentation et les instructions de votre propre fournisseur de messagerie.
Valider l'accès à l'aide de l'analyseur d'accès	Utilisez l'outil Analyseur d'accès pour vous aider à comparer et à analyser les ServiceNow autorisations des utilisateurs, rôles ou groupes sélectionnés. Vous pouvez utiliser ces informations pour résoudre les problèmes d'accès, identifier qui a accès à vos données sensibles et déterminer le niveau d'accès approprié pour les utilisateurs de votre instance. Pour en savoir plus sur les avantages d'Access Analyzer, consultez Exploration de l'analyseur d'accès.

Tableaux de bord sur la posture de sécurité

Utilisez les tableaux de bord personnalisables sur la posture de sécurité à instance unique et multi-instances pour surveiller vos KPI de sécurité. Ces tableaux de bord consolident les informations importantes concernant la sécurité de vos instances dans un seul emplacement et incluent un certain nombre de widgets de tableaux de bord du système de base.

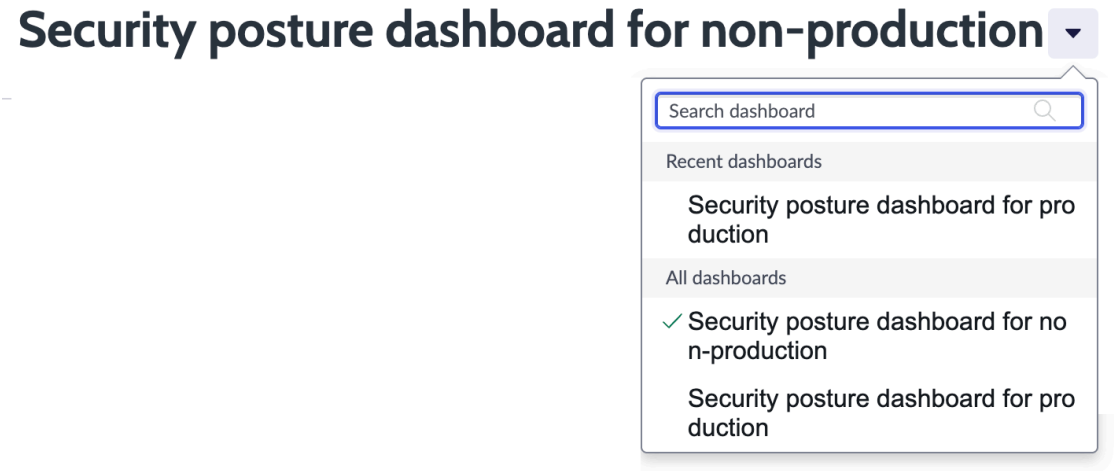
Accéder aux tableaux de bord sur la posture de sécurité

Pour accéder au tableau de bord de la posture de sécurité, ouvrez Centre de sécurité en accédant à **Tous** > **Centre de sécurité**. Sélectionnez **Console de posture de sécurité** dans la section **Consoles de sécurité** . Sur la page **Console de posture de sécurité** , sélectionnez **Tableaux de bord de posture de sécurité** en haut.

Utilisez la flèche vers le bas en regard du **tableau de bord de la posture de sécurité** pour basculer entre les tableaux de bord d'instance.

Traduction automatique

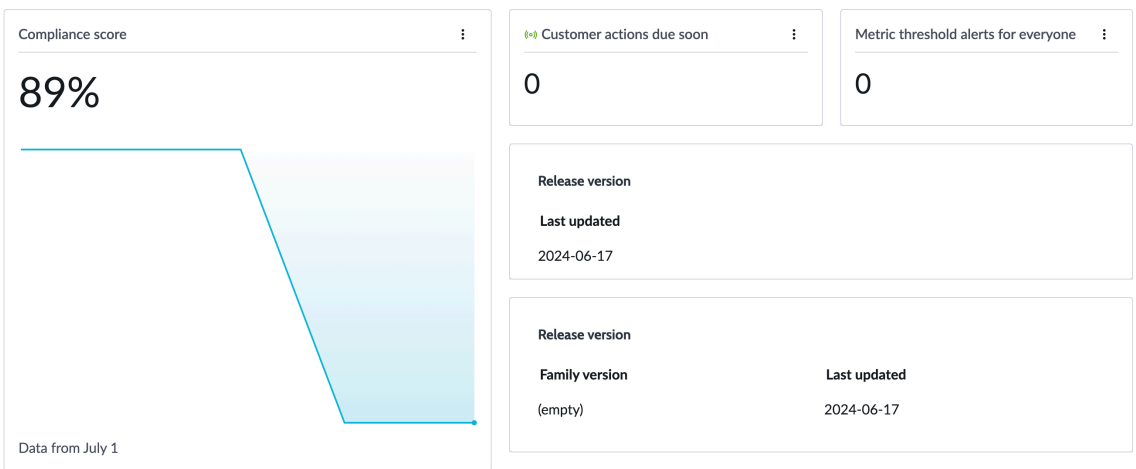
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le tableau de bord est divisé en plusieurs sections contenant des widgets liés à un aspect de la sécurité de l'instance. Sélectionnez un widget sur le tableau de bord pour afficher plus de détails sur cet aspect de la sécurité de votre instance.

En un coup d'œil

At a glance



La section **En un coup d'œil** affiche une vue d'ensemble de la sécurité sur une instance, telle qu'un score de conformité, les actions du client à échéance et les informations sur la version de l'instance.

Score de conformité

Affiche le pourcentage de votre score de conformité d'instance au fil du temps, en commençant par la date semée en bas du widget. Sélectionnez ce widget pour accéder au Tendance du score de conformité à la sécurisation renforcée.

Alertes de seuil de mesure pour moi

Affiche le nombre d'enregistrements d'événements de seuil de mesure [n_vsc_metric_threshold_event] affectés à l'utilisateur actuel. Sélectionnez ce widget pour accéder à une liste de ces enregistrements.

Alertes de seuil de mesure pour tout le monde.

Affiche le nombre d'enregistrements d'événements de seuil de mesure non affectés [n_vsc_metric_threshold_event]. Sélectionnez ce widget pour accéder à une liste de ces enregistrements.

Actions du client à venir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affiche le nombre d’actions client bientôt à échéance. Sélectionnez ce widget pour accéder à Actions du client.

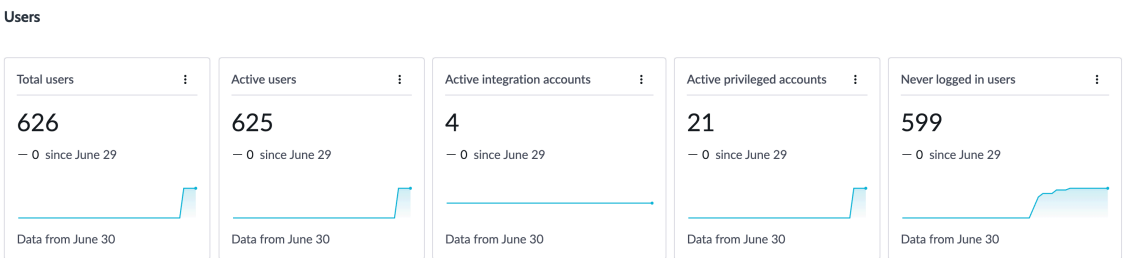
Fichiers téléchargés par l’antivirus

Affiche le nombre de fichiers chargés sur votre instance qui ont été mis en quarantaine. Sélectionnez ce widget pour afficher ces fichiers en quarantaine dans la Antivirus section .Mesures de sécurité

Version de mise en production

Affiche la version familiale de l’instance et la date de la dernière mise à jour de l’instance.

Utilisateurs



La section **Utilisateurs** fournit des informations sur les utilisateurs de votre instance. Les widgets de cette section affichent les informations de l’utilisateur et un graphique linéaire montrant les changements apportés à ces informations au fil du temps. Sélectionnez un widget pour afficher plus de détails.

Total des utilisateurs

Affiche le nombre d’utilisateurs dans votre table Utilisateurs [sys_user]. Sélectionnez ce widget pour afficher les détails de ces enregistrements dans la Sessions actives section Mesures de sécurité.

Utilisateurs actifs

Affiche le nombre d’utilisateurs actifs dans votre table Utilisateurs [sys_user]. Les utilisateurs actifs sont des enregistrements utilisateur dans lesquels le champ **Actif** est sélectionné. Sélectionnez ce widget pour afficher les détails de ces enregistrements dans la Sessions actives section Mesures de sécurité.

Comptes d'intégration actifs

Affiche le nombre de comptes d’intégration dans votre table Utilisateurs [sys_user]. Les comptes d’intégration sont des enregistrements utilisateur dans lesquels le champ **Accès au service Web uniquement** est sélectionné. Sélectionnez ce widget pour afficher les détails de ces enregistrements dans la Sessions actives section Mesures de sécurité.

Comptes privilégiés actifs

Affiche le nombre d’utilisateurs privilégiés actifs dans votre table Utilisateurs [sys_user]. Les utilisateurs privilégiés sont des enregistrements utilisateur dont le champ **Actif** est vrai, **l’utilisateur d’intégration interne** est faux et **l’utilisateur d’intégration interne** est inactif. Sélectionnez ce widget pour afficher les détails de ces enregistrements dans la Sessions actives section Mesures de sécurité.

Utilisateurs jamais connectés

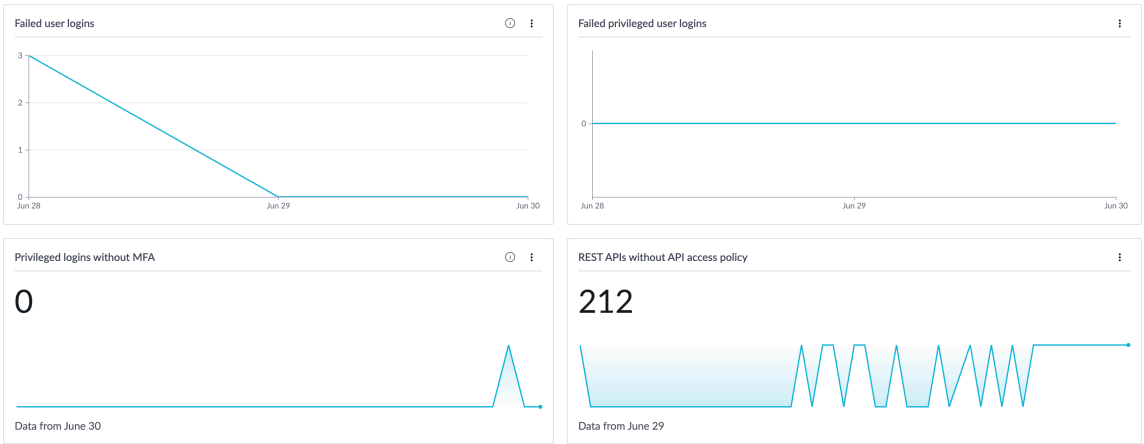
Affiche le nombre d’utilisateurs dans votre table Utilisateurs [sys_user] créée au cours des 60 derniers jours et n’ayant aucune valeur dans le champ Heure de la **dernière connexion** . Sélectionnez ce widget pour afficher les détails de ces enregistrements dans la Sessions actives section Mesures de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Protection de connexion

Login protection



La section **Protection des connexions** comprend des informations sur les échecs de connexion, y compris les échecs de tentatives de connexion pour les utilisateurs privilégiés. Ces widgets incluent un graphique linéaire montrant les changements apportés à ces informations au fil du temps. Sélectionnez un widget pour afficher plus de détails.

Échecs de connexion des utilisateurs

Affiche le nombre de tentatives de connexion utilisateur échouées. Sélectionnez ce widget pour naviguer afin d'afficher les détails des échecs de connexion dans Mesures de sécurité.

Échec des connexions d'utilisateurs privilégiés

Affiche le nombre d'échecs de tentatives de connexion utilisateur à partir de comptes privilégiés. Les utilisateurs privilégiés sont des enregistrements utilisateur dont le champ **Actif** est vrai, **l'utilisateur d'intégration interne** est faux et **l'utilisateur d'intégration interne** est inactif. Sélectionnez ce widget pour naviguer afin d'afficher les détails des échecs de connexion dans Mesures de sécurité.

Connexions privilégiées sans MFA

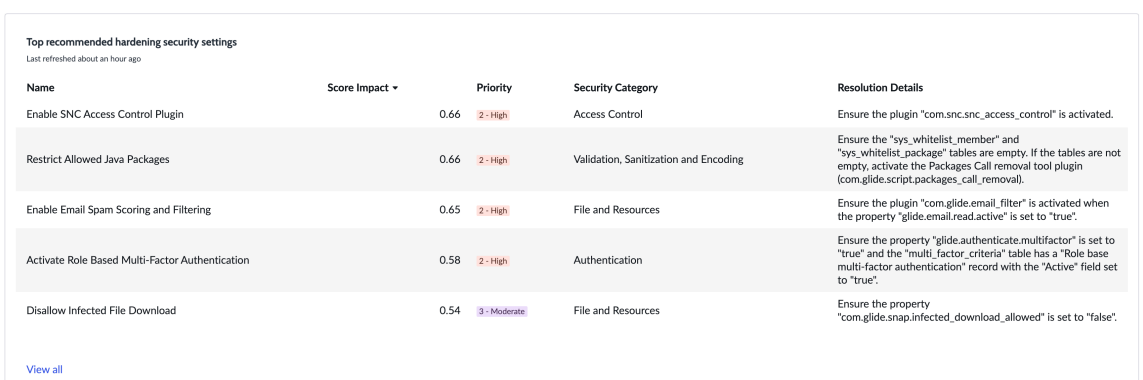
Affiche le nombre de comptes privilégiés qui ne sont pas configurés pour l'authentification multifacteur (MFA). Sélectionnez ce widget pour accéder à une liste de ces comptes dans Mesures de sécurité.

API REST sans politique d'accès à l'API

Affiche une liste des API REST qui ne sont pas restreintes par une politique d'accès API. Sélectionnez ce widget pour accéder à une liste de ces API REST dans Mesures de sécurité.

Sécurisation renforcée de l'instance

Instance hardening

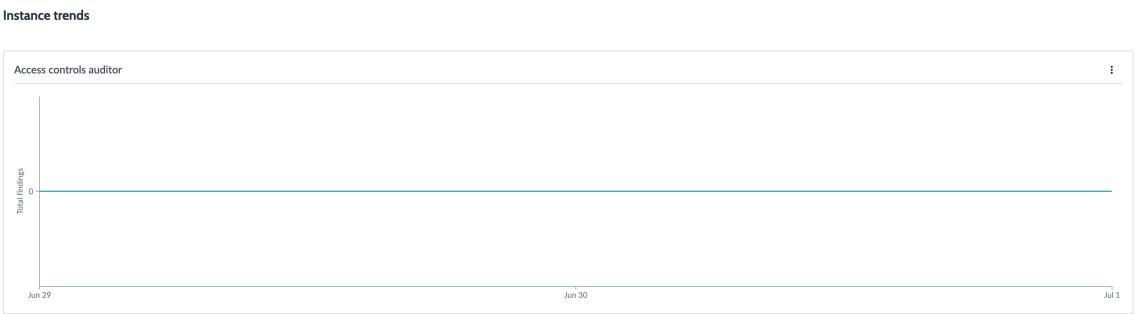


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

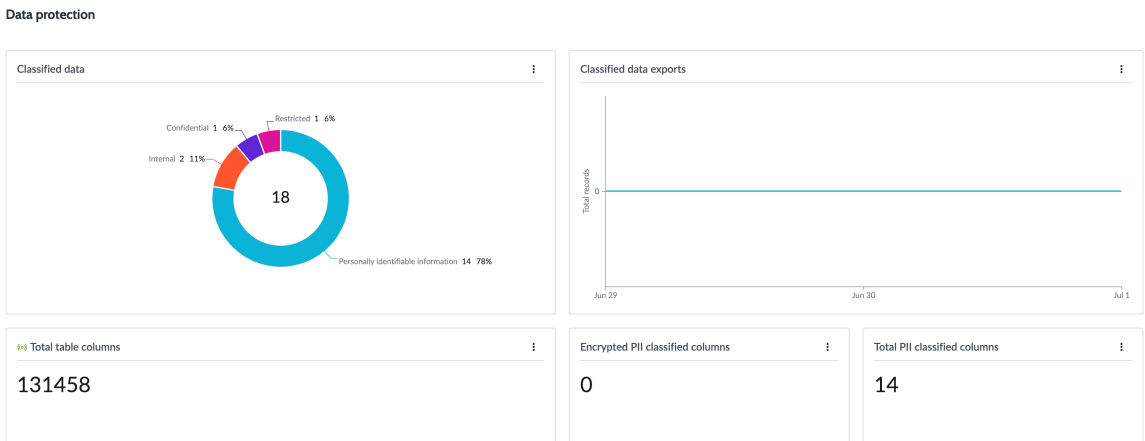
La section **Sécurisation renforcée de l'instance** contient les paramètres de sécurité de sécurisation renforcée recommandés que vous pouvez modifier pour améliorer la sécurité de l'instance. Utilisez cette section pour voir la priorité et l'impact potentiel de ces changements.

Tendances d'instances



Le tableau de bord **Tendances d'instance** affiche les résultats de la suite d'analyse de l'auditeur des contrôles d'accès.

Protection des données



Utilisez la section **Protection des données** pour afficher une vue d'ensemble des données classifiées, telles que les informations personnelles identifiables (PII). Le tableau de bord suit également les exportations de données classifiées.

Données classifiées

Affiche un graphique circulaire des données classifiées sur votre instance, séparées par type. Sélectionnez une section du graphique pour afficher les détails de ces enregistrements. Pour plus d'informations sur la classification des données, reportez-vous à la section Classification des données.

Exportations de données classées

Affiche le nombre d'enregistrements classifiés qui ont été exportés à partir de votre instance. Sélectionnez ce widget pour afficher une liste des exportations classées dans la Exporter section .Mesures de sécurité

Colonnes de la table des totaux

Affiche un nombre de toutes les colonnes (champs) dans les tables de votre instance. Sélectionnez ce widget pour examiner ces colonnes dans la Classification des données section .Mesures de sécurité

Colonnes classifiées PII chiffrées

Traduction automatique

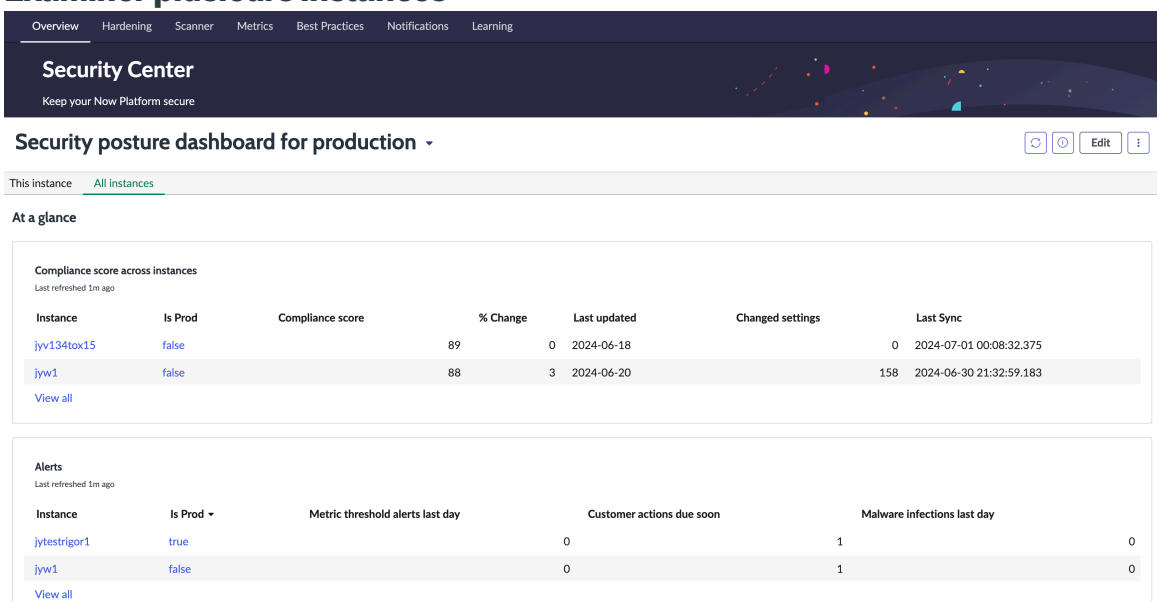
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affiche un nombre d'enregistrements chiffrés classifiés comme informations personnellement identifiables (IPI). Sélectionnez ce widget pour examiner ces enregistrements dans la Classification des données section de Mesures de sécurité.

Nombre total de colonnes classifiées PII

Affiche un nombre de tous les enregistrements classifiés comme informations personnellement identifiables (PII). Sélectionnez ce widget pour examiner ces enregistrements dans la Classification des données section de Mesures de sécurité.

Examiner plusieurs instances



Consultez la posture de sécurité de vos instances de non-production sans quitter votre instance de production à l'aide de l'onglet **Toutes les instances** en haut du tableau de bord. L'onglet **Toutes les instances** affiche une version condensée des mêmes informations que l'onglet **Cette instance** , mais inclut également les données de toutes vos instances de non-production.

Par défaut, l'onglet **Toutes les instances** affiche des informations sur l'instance de production à laquelle vous êtes connecté et toutes les instances de non-production dans tous vos environnements de production.

Vous pouvez ajouter ou supprimer des instances qui apparaissent sur ce tableau de bord en modifiant votre configuration d'approbation. Fournir une visibilité des données entre les instances permet de les afficher dans votre tableau de bord. Pour obtenir des détails sur ce processus, consultez Basic trust configuration for data sync applications .

Personnalisation du tableau de bord

Le tableau de bord de la posture de sécurité de l'instance ne peut pas être personnalisé, mais vous pouvez dupliquer le tableau de bord en sélectionnant l'icône **Actions supplémentaires** (Actions ⋮) et en sélectionnant **Dupliquer**. Vous pouvez modifier le tableau de bord en double.

Tâches de sécurité

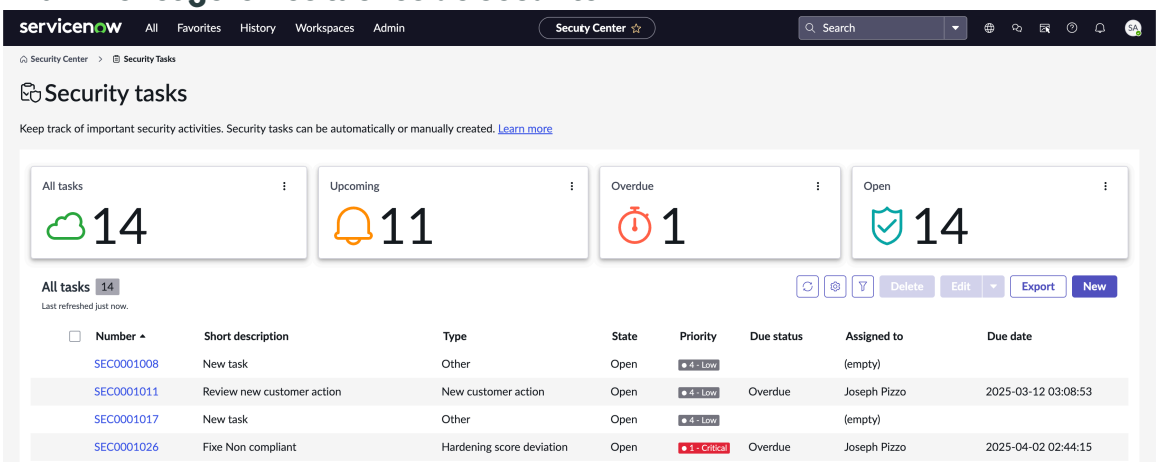
Utilisez les tâches de sécurité pour surveiller, classer par ordre de priorité et affecter toutes vos tâches liées à la sécurité au même endroit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gagnez du temps en suivant et en organisant toutes les tâches nécessaires pour améliorer et maintenir la posture de sécurité de votre instance à l'aide de tâches de sécurité.

Examiner et gérer les tâches de sécurité



Accéder aux tâches de sécurité en accédant à **Tous** > **Centre de sécurité** > **Tâches de sécurité**. Par défaut, toutes les tâches sont affichées dans la liste. Vous pouvez facilement filtrer les tâches à venir, en retard ou ouvertes en sélectionnant les cartes au-dessus de la liste. Ces cartes affichent également le nombre actuel de tâches dans chacune de ces catégories. Vous pouvez affiner davantage votre filtre en utilisant les options de filtrage des champs de table normales, puis en sélectionnant le bouton de filtre ( ), puis en sélectionnant le bouton Vue avancée pour créer et enregistrer des filtres personnalisés à utiliser ultérieurement.

Rôles d'utilisateur

Les tâches de sécurité utilisent les rôles suivants :

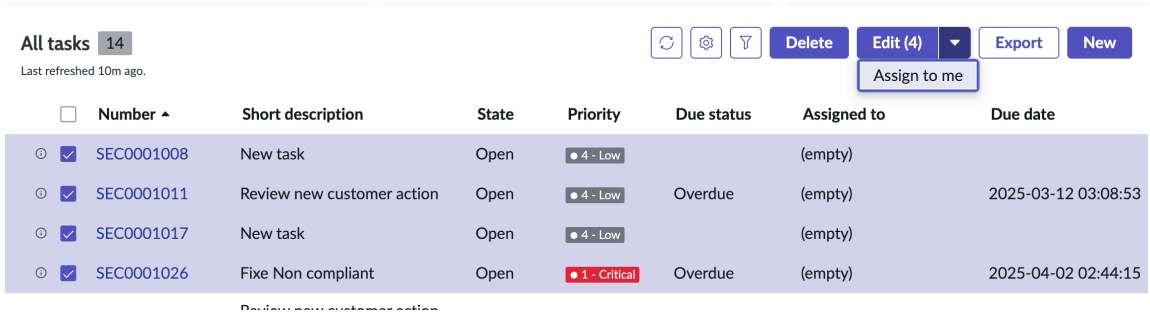
Utilisateur	Rôle requis	Description
Administrateur système	administrateur	Les administrateurs système peuvent afficher, créer, affecter et supprimer des tâches de sécurité.
Visionneuse du centre de sécurité	sn_vsc_security_center_viewer	Les visionneuses peuvent afficher, mais pas créer, supprimer ou modifier les tâches de sécurité.
Gestionnaire des tâches de sécurité	sn_vsc_task_manager	Les gestionnaires de tâches de sécurité peuvent travailler sur les tâches affectées, afficher les pages associées au gestionnaire de tâches et créer et gérer des tâches dans le centre de sécurité. Ils peuvent afficher les tâches affectées à d'autres utilisateurs, mais ne peuvent pas modifier les tâches affectées à d'autres utilisateurs. Les gestionnaires de tâches ne peuvent pas accéder aux pages autres que celles du gestionnaire de tâches dans le centre de sécurité.
ITIL	itil	Les utilisateurs ITIL peuvent interagir avec les tâches de sécurité qui leur sont affectées, mais ne peuvent pas afficher toutes les tâches comme les rôles d'administrateur et de gestionnaire des tâches de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous affecter rapidement des tâches de sécurité

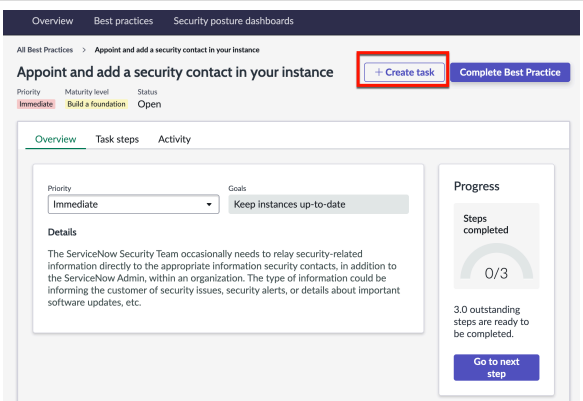
Utilisez les cases à cocher situées à gauche des éléments de la liste pour sélectionner plusieurs éléments. Lorsque l'une des tâches est sélectionnée, vous pouvez utiliser le bouton **Supprimer** pour supprimer les tâches sélectionnées ou le bouton **Modifier** pour vous affecter les tâches sélectionnées.

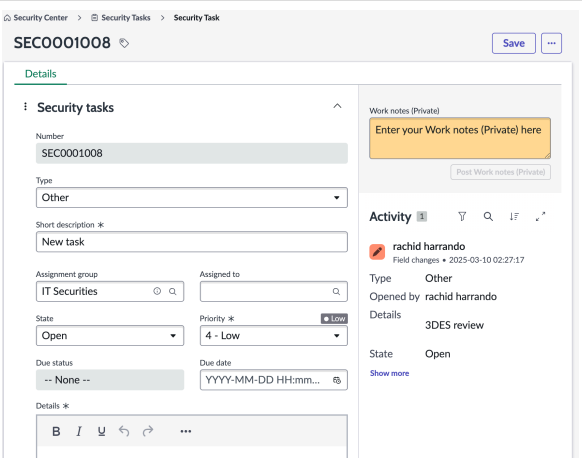


Créer des tâches de sécurité

Créez une tâche de sécurité avec le bouton **+Créer une tâche** , disponible sur différentes pages de sécurité de la plateforme.

Par exemple, dans Centre de sécurité, sur la page des détails de l'outil Bonnes pratiques, l'administrateur peut sélectionner le bouton **+Créer une tâche** pour créer et affecter une tâche afin de respecter cette bonne pratique.





Tâches générées automatiquement

Les tâches de sécurité peuvent être générées automatiquement. La génération automatique de tâches de sécurité est déclenchée par un événement associé qui s'est produit sur la plateforme. Pour en savoir plus sur les tâches de sécurité générées, consultez .Génération automatique de tâches de sécurité

Modifier et affecter des tâches de sécurité

Modifiez les tâches de sécurité pour les affecter à des utilisateurs, définir des dates d'échéance et fournir des détails supplémentaires aux utilisateurs qui effectueront ces tâches. Pour plus de détails, voir Modifier les tâches de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exporter les tâches

Vous pouvez exporter des tâches de sécurité au format de votre choix. Pour plus de détails, voir Exporter des tâches de sécurité.

Génération automatique de tâches de sécurité

Découvrez comment et quand votre instance génère des tâches de sécurité.

Tâches de sécurité générées automatiquement

Les tâches de sécurité peuvent être générées automatiquement. La génération automatique de tâches de sécurité est déclenchée par un événement associé qui s'est produit sur la plateforme. Par exemple :

Seuil des mesures dépassé

Une tâche de sécurité est générée pour une mesure lorsque son seuil est dépassé. Il n'y a qu'une seule tâche ouverte pour une mesure, même si la même mesure comporte plusieurs violations. Si une tâche de sécurité pour une mesure non respectée est fermée, une nouvelle tâche est générée si le seuil est à nouveau atteint.

Notifications des événements

Une tâche de sécurité est générée lorsqu'une notification d'événement de sécurité se déclenche (respecte les conditions de sa politique). Comme pour les mesures, il n'y a qu'une seule tâche ouverte pour une politique, avec une nouvelle tâche générée si la précédente est fermée et que la notification se déclenche à nouveau. Pour en savoir plus sur les notifications d'événements de sécurité, reportez-vous à la section Notifications des événements de sécurité.

Écart du score de sécurisation renforcée

Lorsque le score de sécurisation renforcée se dégrade en dessous de la valeur de seuil configurée (3 par défaut), une tâche de sécurité est générée. Par exemple, si le score de sécurisation renforcée est de 97 et de 94 le lendemain, une tâche de sécurité est créée juste après le calcul du score de 94. Une seule tâche ouverte est créée. La plateforme ne générera pas d'autre tâche si le score redescend le lendemain de 94 à 91. Pour plus d'informations sur votre score de sécurisation renforcée, reportez-vous à la section Tendance du score de conformité à la sécurisation renforcée.

Action du client

Une tâche de sécurité est générée chaque fois qu'une action du client est installée. Pour plus d'informations sur les actions du client, reportez-vous à la section Actions du client.

Annonce de bannière

Une tâche de sécurité est générée pour chaque nouvelle annonce de bannière. Pour en savoir plus sur les annonces de bannières, reportez-vous à la section Annonces de bannières de sécurité.

Paramètres de sécurité générés automatiquement

Les options de configuration des tâches de sécurité générées automatiquement se trouvent dans la page des propriétés du centre de sécurité. Recherchez ces paramètres en accédant à **Tous** > **Centre de sécurité** > **Propriétés du centre de sécurité**.

Activer/désactiver les tâches de sécurité automatisées

Lorsque le champ **Oui/Non** est sélectionné, les tâches de sécurité automatisées sont activées sur votre instance.

Seuil de dégradation du score de sécurisation renforcée

La valeur du champ représente la dégradation du score de sécurisation renforcée (depuis le dernier score quotidien) pour générer une tâche de sécurité. Cette valeur doit être un nombre entier positif. La valeur par défaut est de 3.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modifier les tâches de sécurité

Découvrez comment créer, modifier, supprimer ou exporter des tâches de sécurité dans le centre de sécurité

Avant de commencer

Rôle requis : admin ou sn_vsc_task_manager

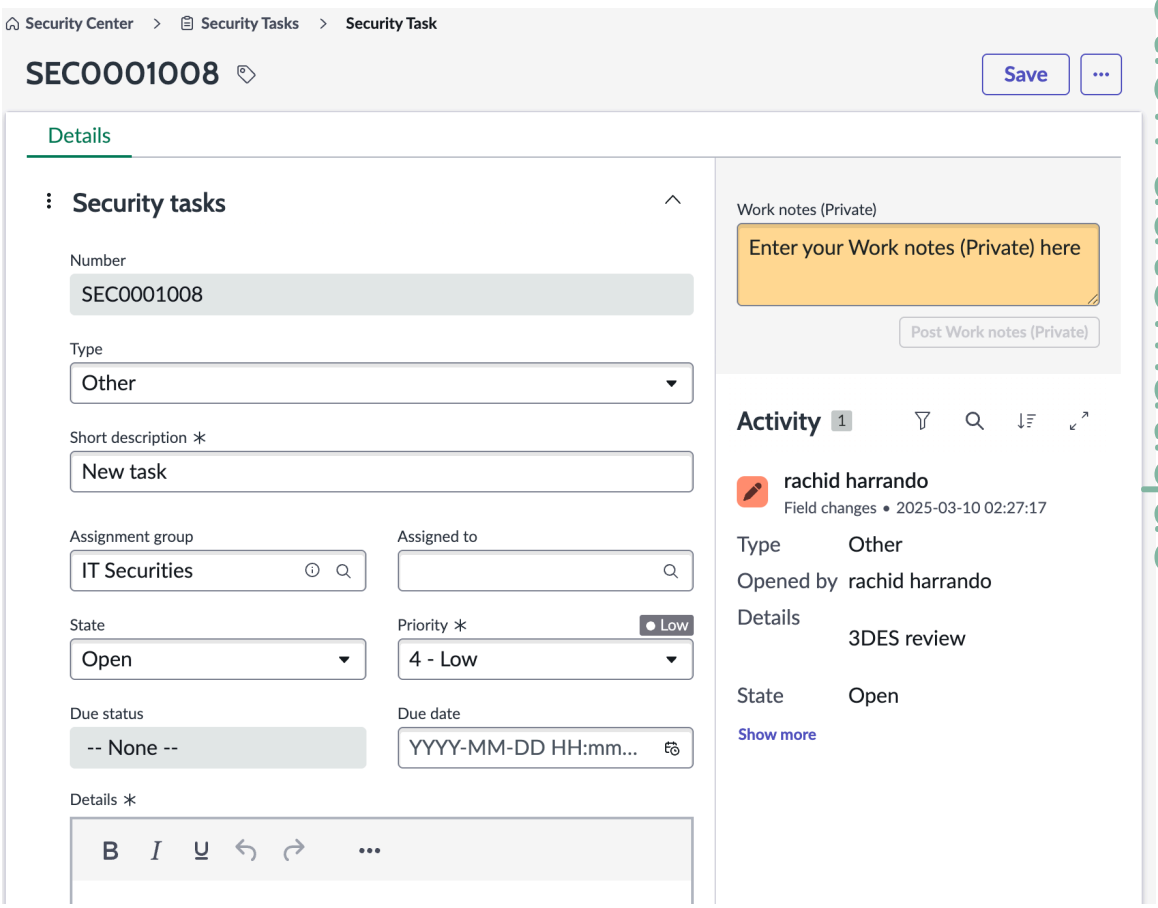
Procédure

1. Accéder à votre liste de tâches de sécurité en accédant à **Tous** > **Centre de sécurité** > **Tâches de sécurité**.
2. Dans la liste Tâches de sécurité, vous pouvez modifier vos tâches de sécurité de deux manières :

Modifier dans le formulaire Tâche de sécurité

Sélectionnez un numéro de tâche de sécurité dans la liste pour ouvrir l'enregistrement de tâche de sécurité et afficher ses détails. Ici, vous pouvez modifier, affecter à un autre utilisateur et ajouter des notes de travail.

Important :
N'oubliez pas que les utilisateurs auxquels des tâches sont affectées doivent être administrateurs ou avoir le rôle sn_vsc_task_manager.

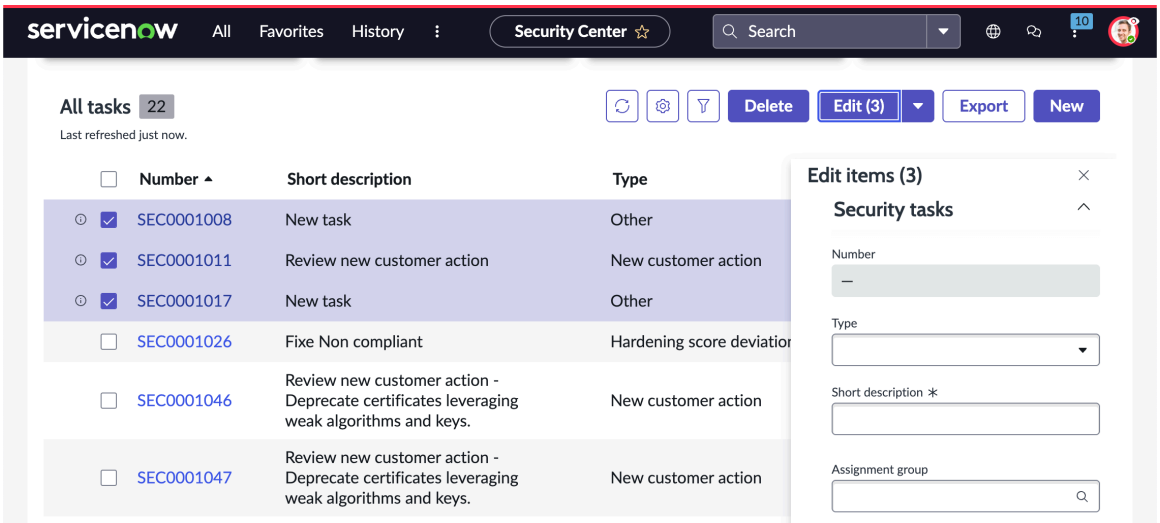


Modifier à partir de la liste de tâches de sécurité

Sélectionnez une ou plusieurs tâches de sécurité en cochant la case située à gauche, puis sélectionnez le bouton **Modifier** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Renseignez les champs selon vos besoins :

Champ	Description
Numéro	Numéro généré automatiquement utilisé pour identifier la tâche
Type	Sélectionnez un type de tâche : ○ Seuil des mesures dépassé ○ Nouvelle action du client ○ Notifications des événements ○ Écart du score de sécurisation renforcée ○ Nouvelle annonce de bannière
Description brève	Brève description de la tâche
Groupe d'affectation	Groupe d’affectation pour la tâche
Affecté à	Personne affectée à la tâche. Cet utilisateur doit faire partie du groupe d’affectation sélectionné dans le champ **Groupe d’affectation** et avoir le *admin* rôle ou *sn_vsc_task_manager* .
État	État de la tâche : ○ En attente ○ En cours ○ En cours ○ Fermé ○ Annulé
Priorité	Priorité de la tâche : ○ 1 - Critique ○ 2 : élevé ○ 3 - Modéré ○ 4 : faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Statut de l'échéance	Indique si la tâche est **à venir** ou **en retard**, en fonction de la date indiquée dans le champ Date **d'échéance** .
Date d'échéance	Date et heure auxquelles la tâche doit être terminée.
Détails	Utilisé pour fournir des détails, des liens ou d'autres informations que les utilisateurs doivent connaître sur cette tâche.
Notes de travail	Notes sur cette tâche. Les notes saisies dans ce champ sont horodatées et affichées sur la liste des activités à droite de l'écran.
Notes de travail (privées)	Vous pouvez ajouter des notes de travail en privé en les saisissant dans ce champ et en sélectionnant le bouton **Publier les notes de travail (privées).**

4. Sélectionnez **Enregistrer** pour enregistrer l'enregistrement de la tâche de sécurité. Si vous modifiez un enregistrement de la liste, sélectionnez **Mettre à jour**.
5. **Facultatif :** Si nécessaire, vous pouvez supprimer une tâche de la liste en cochant sa case à droite, puis en sélectionnant **Supprimer**, ou dans le formulaire en sélectionnant l'icône Plus (...), puis en sélectionnant **Supprimer**.

Exporter des tâches de sécurité

Découvrez comment exporter des tâches de sécurité dans des fichiers que vous pouvez télécharger et utiliser dans d'autres logiciels.

Avant de commencer

Rôle requis : admin

Procédure

1. Accéder à votre liste de tâches de sécurité en accédant à **Tous** > **Centre de sécurité** > **Tâches de sécurité**.
2. Sélectionnez une ou plusieurs tâches de sécurité en cochant la case correspondante située à gauche
3. Sélectionnez le bouton **Exporter** .
4. Sous **Type de fichier**, sélectionnez le format de fichier vers lequel vous souhaitez exporter les tâches de sécurité.
   Vous pouvez choisir parmi les formats Excel, CSV, JSON ou PDF.
5. Sous **Type de livraison**, sélectionnez **Télécharger** ou **E-mail**.

   Télécharger

   Le fichier d'exportation est téléchargé à l'aide de votre navigateur.

   E-mail

   Le champ **E-mail** s'affiche. Entrez une adresse **e-mail dans le champ E-mail** , et le fichier d'exportation est envoyé à l'adresse e-mail spécifiée.

Apprentissage de la sécurité

Accédez aux supports d'apprentissage sur la sécurité à partir d'une seule page.

Lisez des livres blancs sur la sécurité, des ebooks, des articles de base de connaissances, de la documentation produit et des discussions de la communauté à partir d'une vue consolidée en accédant à **Apprentissage**. Le contenu est organisé par en-têtes et cartes

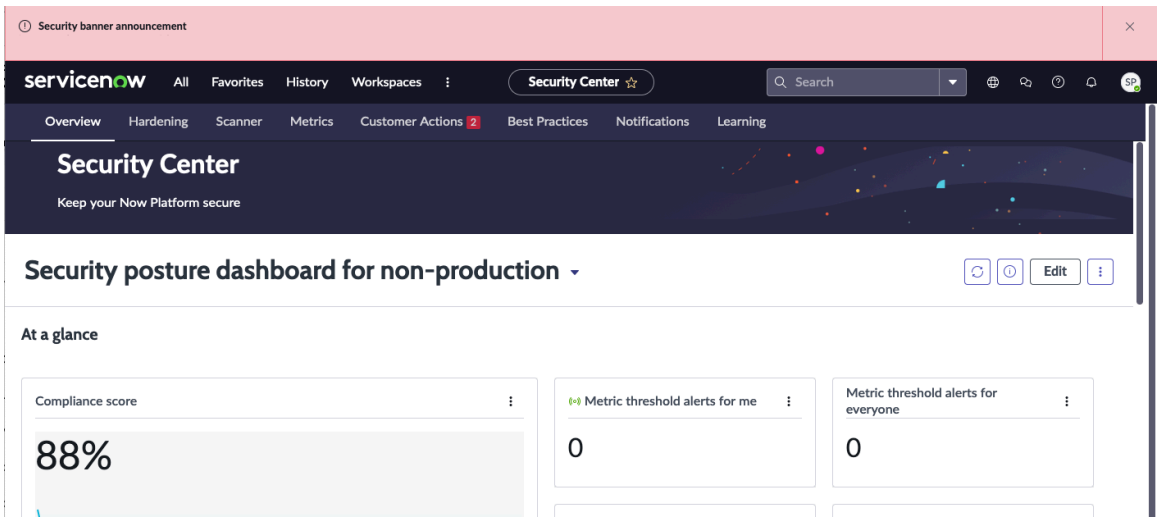
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'interface utilisateur descriptives pour vous permettre d'identifier rapidement la ressource appropriée.

Annonces de bannières de sécurité

Activez les annonces de bannières de sécurité pour rester informé des alertes de sécurité urgentes et critiques à l'aide de bannières haute visibilité visibles par les administrateurs dans l'interface utilisateur de l'instance.

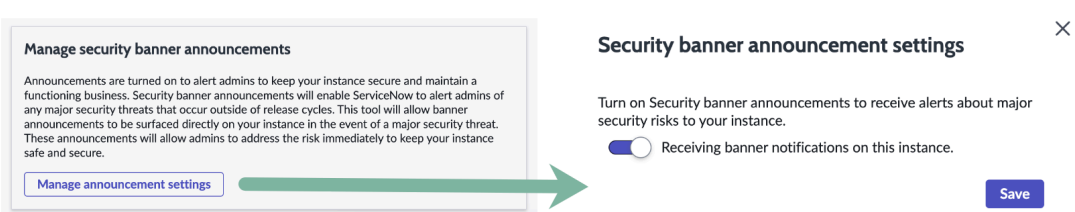


Les annonces de bannières de sécurité sont des annonces affichées aux administrateurs client, envoyées par ServiceNow pour vous tenir informé des correctifs pour les menaces de sécurité potentielles qui ont été découvertes récemment. Ces alertes contiennent un résumé du risque de sécurité et incluent un lien vers lequel vous pouvez en savoir plus et agir pour sécuriser votre instance.

Les administrateurs peuvent fermer la bannière en sélectionnant le bouton fermer (x), mais la bannière réapparaît à chaque nouvelle session jusqu'à ce que la date d'expiration de la bannière soit dépassée. Les administrateurs peuvent désactiver les annonces de bannières en définissant la valeur de la propriété système sn_vsc.configure_customer_push_action sur faux.

Activer ou désactiver les annonces de bannières de sécurité

La fonctionnalité de bannière de sécurité est activée par défaut. Pour activer ou désactiver les annonces de bannières de sécurité, accédez à **Sécurité de système** > **Centre de sécurité** > **Notifications**. Sur cette page, sélectionnez le bouton **Gérer les paramètres des annonces** .



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Centre de sécurité de l'instance

Surveillez le niveau de conformité des contrôles de sécurité de l’instance, affichez les mesures de surveillance des événements de sécurité et configurez et gérez les paramètres de sécurité de l’instance à partir du Centre de sécurité de l’instance. Centre de sécurité de l’instance consolide plusieurs composants de sécurité clés dans une console de contrôle unique qui vous aide à détecter, protéger et répondre aux événements de sécurité basés sur l’instance.

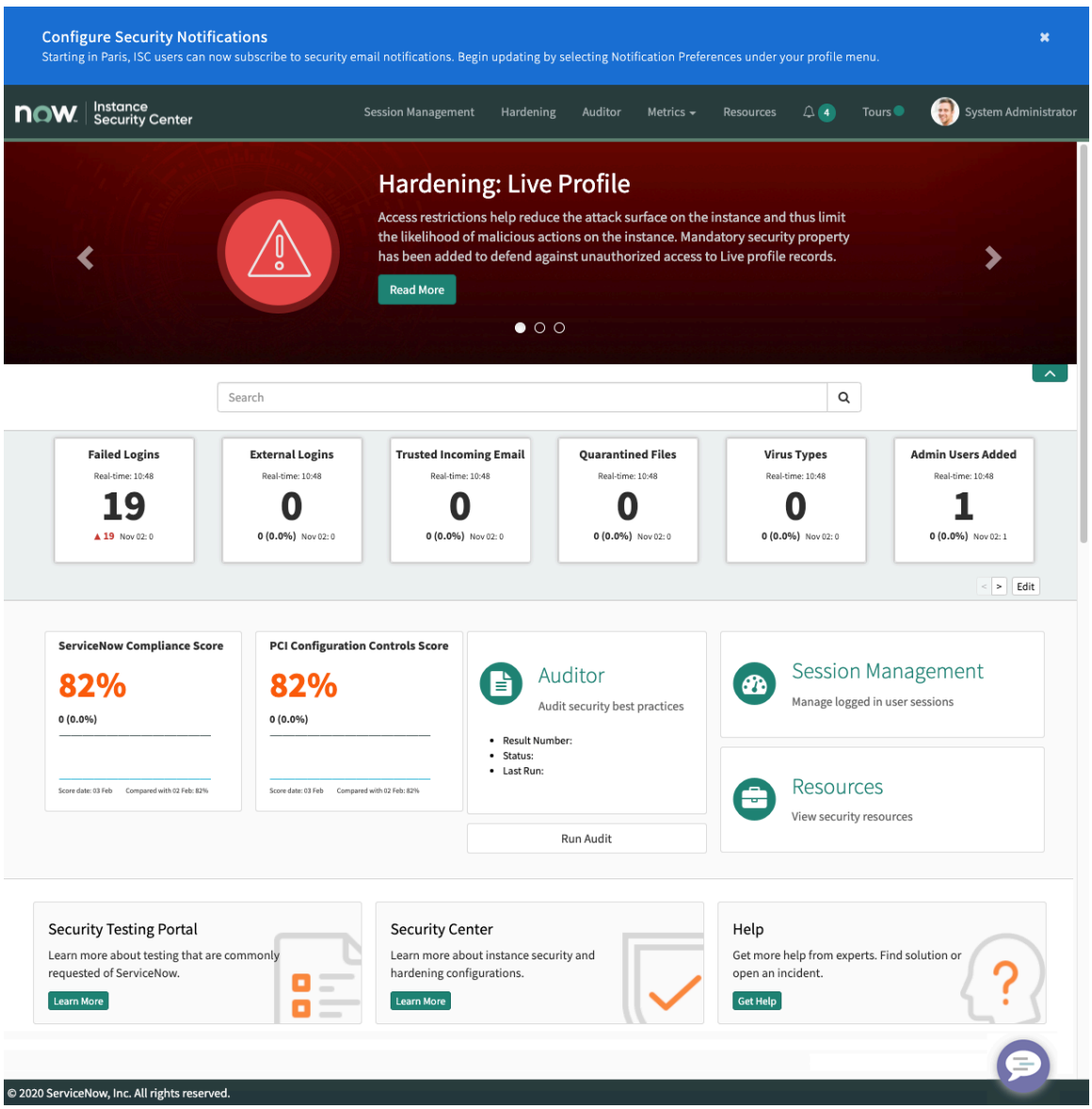
Important :

Le centre de sécurité de l’instance (ISC) a atteint la fin des ventes en septembre 2024 et n’est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l’avenir. Pour plus d'informations, consultez Centre de sécurité de l’instance vers la ServiceNow Centre de sécurité migration.

Composants du Centre de sécurité de l’instance

Pour accéder au Centre de sécurité de l’instance, accédez à **Sécurité de système** > **Centre de sécurité de l'instance** ou la page d’accueil Administration système.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page d'accueil du Centre de sécurité de l'instance contient les composants de sécurité suivants :

- Messages de l'administrateur
- Bannière de sécurité rotative
- Rechercher
- Ruban d'événement de sécurité
- Score de conformité quotidien
- Score des contrôles des configurations PCI
- Gestion des sessions
- Sécurisation renforcée
- Auditeur
- Mesures (utilisateur, e-mail et antivirus)
- Ressources
- Notifications de sécurité
- Visites guidées
- Portail de test de la sécurité
- Centre de sécurité
- Aide
- Accès à Agent virtuel

À partir de la page d'accueil du Centre de sécurité de l'instance, vous pouvez afficher le score de conformité de sécurité de votre instance et surveiller son intégrité de sécurité globale. Vous pouvez ensuite configurer ou mettre à jour les propriétés système liées à la sécurité de votre instance afin qu'elles soient conformes aux exigences de sécurité.

Remarque :
Le Centre de sécurité de l'instance ne prend pas en charge Séparation de domaine.

Rôles d'utilisateur

Pour utiliser Centre de sécurité de l'instance, vous devez avoir le rôle administrateur ou security_dashboard_user.

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

roles

Rôle requis	Utilisateur	Avantages
administrateur	Ce rôle a accès à l'ensemble des fonctionnalités, fonctions et données système, car les administrateurs peuvent remplacer les règles de liste de contrôle d'accès (ACL) et subir avec succès toutes les vérifications de rôles.	Utilisez Centre de sécurité des outils pour améliorer la posture de sécurité de l'instance et surveiller les comportements liés à la sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

roles (suite)

Rôle requis	Utilisateur	Avantages
	Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus ciblés sont disponibles.	
sn_vsc.security_center_viewer	Ce rôle permet aux utilisateurs qui ne sont pas administrateurs d'afficher les informations dans Centre de sécurité les outils, mais sans pouvoir y apporter de modifications ou modifier les configurations d'instance Centre de sécurité en tirant parti des Centre de sécurité outils. Par exemple, les propriétaires de plateformes, les analystes des opérations de sécurité ou les personnes concernées par la conformité peuvent vouloir ou avoir besoin de consulter certains des KPI de sécurité, des informations de sécurité et du matériel d'apprentissage sur la sécurité disponibles dans Centre de sécurité.	Gagnez en visibilité sur Centre de sécurité les outils permettant de surveiller la posture de sécurité de l'instance et de surveiller les comportements de sécurité.

Avertissement :
Pour vous assurer que le Centre de sécurité de l'instance reçoit des informations de sécurité à jour à chaque mise à niveau, ne personnalisez pas ce module. Si vous modifiez des paramètres de sécurité sur votre instance, assurez-vous de les tester d'abord dans un environnement de non-production.

Messages de l'administrateur

Des messages et des rappels, destinés principalement aux administrateurs, apparaissent au-dessus de la bannière de sécurité tournante.

Par exemple, un message Configurer les notifications de sécurité s'affiche pour rappeler aux administrateurs de configurer les préférences des notifications de sécurité s'ils ne l'ont pas encore fait. Cela les dirige également vers la bonne page pour le faire.

Remarque :
La bannière des messages administrateur n'apparaît pas pour les utilisateurs non-administrateurs ou s'il n'existe aucun élément actionnable pour les utilisateurs administrateurs.

Bannière de sécurité rotative

Pour vous aider à surveiller l'intégrité de sécurité de votre instance, les messages de sécurité de l'instance critique s'affichent dans la bannière rotative.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Deux à trois messages de sécurité tournent normalement à intervalles réguliers.
- Les points au bas de la bannière vous indiquent le nombre total de messages de sécurité actuels.
- Pour les parcourir, sélectionnez les points ou sélectionnez les flèches qui apparaissent de chaque côté des messages.

Les couleurs d'arrière-plan des bannières indiquent la gravité relative des messages.

Couleur	Description
Rouge	Situation de sécurité critique nécessitant une réponse rapide ou une recommandation sur la façon de protéger ou de répondre aux événements de sécurité critiques.
Gris foncé	Message d'avertissement non critique.
Bleu	Message d'information générale.

Pour réduire ou réduire le contenu textuel de la bannière, sélectionnez . Pour agrandir le contenu du texte, sélectionnez-le à nouveau.

- Lorsque vous utilisez à nouveau Centre de sécurité de l'instance, le contenu textuel apparaît comme réduit ou développé, selon la façon dont vous l'avez utilisé lors de votre session précédente.
- Si le contenu textuel lui-même change, il apparaît comme agrandi pour tous les utilisateurs.

Rechercher

Utilisez la barre de recherche pour rechercher dans l'ensemble du centre de sécurité de l'instance des ressources de sécurité qui vous aident à comprendre et à résoudre les problèmes de sécurité. Vous pouvez rechercher les ressources liées à la sécurité suivantes :

- Now Support Base de connaissances des articles
- Pages du Centre de sécurité de l'instance
- Liens externes Now Support
- Les widgets de sécurité PA, tels que le score de conformité quotidien et les e-mails entrants externes
- Contenu de la bannière

Ruban d'événement

Utilisez le ruban d'événement pour afficher les mesures clés de surveillance des événements de sécurité pour l'instance actuelle.

- Pour faire défiler manuellement les mesures, sélectionnez les flèches vers la droite ou vers la gauche.
- Pour configurer le ruban d'événement, sélectionnez **Modifier**.

Pour en savoir plus sur le ruban d'événement et sa configuration, reportez-vous aux rubriques Surveiller les événements de sécurité et Configurer le ruban d'événement de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score de conformité quotidien

La section Score de conformité quotidien contient les tuiles **Score de conformité quotidien**, **Gestion des sessions**, **Sécurisation renforcée**, **Auditeur** et **Ressources** .

Vous utilisez le score de conformité quotidien pour évaluer l'intégrité de votre instance du point de vue de la sécurité.

Le score de conformité quotidien est un score en pourcentage. Elle est basée sur le degré de conformité des paramètres actuels de vos propriétés de sécurité d'instance avec les valeurs de conformité publiées dans le Paramètres de sécurisation renforcée.

- Pour en savoir plus sur les calculs quotidiens du score de conformité et sur l'impact des paramètres de sécurisation renforcée, reportez-vous à la section Vérifier le score de conformité quotidien et configurer les paramètres des propriétés de sécurité.
- Le bouton **Actualiser** permet à un administrateur de recalculer instantanément le score de conformité quotidien. Pour en savoir plus, consultez Actualisation quotidienne des données de score, de tendance et de graphique de conformité.

Sécurisation renforcée

Utilisez ce processus pour ajuster les propriétés de configuration de sécurité spécifiques qui affectent le score de conformité quotidien :

1. Pour accéder à la page Configurations de la conformité à la sécurisation renforcée et effectuer la sécurisation renforcée de la sécurité de l'instance, sélectionnez la vignette du **score de conformité quotidienne** ou le lien **de sécurisation renforcée** .
2. Indiquez si vous souhaitez afficher tous les contrôles de sécurité recommandés ou uniquement les contrôles de sécurité recommandés. Sélectionnez ensuite la catégorie dans laquelle vous souhaitez travailler.
3. Définissez chaque propriété de configuration de sécurité dans la catégorie sélectionnée. Cliquez sur **Plus d'informations** pour afficher des informations détaillées sur une propriété.

Pour en savoir plus sur le renforcement et l'optimisation des propriétés de configuration de sécurité afin d'accroître la conformité, reportez-vous à la section Ajuster les paramètres de sécurité de l'instance pour accroître la conformité.

Pour en savoir plus sur l'actualisation des données de tendance et de graphique, reportez-vous à la section Actualisation quotidienne des données de score, de tendance et de graphique de conformité.

Auditeur

Exécutez l'auditeur pour analyser votre instance et trouver des définitions de sécurité incorrectes. Elle fournit des résultats que vous pouvez corriger pour améliorer la posture de sécurité de votre instance.

Pour accéder à la page Auditeur, sélectionnez la vignette **Auditeur** ou le lien **Auditeur** . Pour en savoir plus, consultez Rechercher des définitions de sécurité incorrectes.

Gestion des sessions

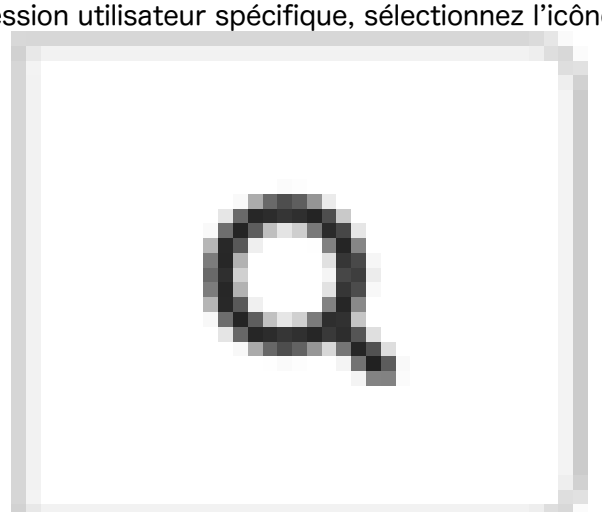
Utilisez Gestion des sessions pour :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez et gérez les sessions de connexion de l'utilisateur.
- Consultez la session de connexion de l'utilisateur du nœud actuel auquel vous êtes connecté.
- Consultez les informations détaillées sur chaque session, telles que le nom d'utilisateur et l'adresse IP.
- Isolez et verrouillez des sessions utilisateur spécifiques qui présentent des risques de sécurité.

Pour accéder à la page Gestion des sessions, sélectionnez la vignette ou le lien **Gestion des sessions** .

Champ	Description
Utilisateur	Nom de l'utilisateur associé à cette session de connexion. • Pour localiser une session utilisateur spécifique, sélectionnez l'icône de recherche spotlight () pour effectuer une recherche par utilisateur, par mot clé d'agent utilisateur ou par adresse IP. Par exemple, si vous souhaitez trouver toutes les connexions actuelles à partir d'un type spécifique de navigateur, entrez le nom du navigateur comme mot clé dans le champ **Agent d'utilisateur** . • Cliquez sur un nom d'utilisateur pour accéder à l'enregistrement du profil d'utilisateur. Vous pouvez modifier le profil d'utilisateur uniquement si un rôle administrateur vous est affecté. **Remarque :** Pour en savoir plus sur les profils d'utilisateur, consultez Créer un utilisateur .
MFA	Cochez la case indiquant si l'authentification multifacteur (MFA) est activée pour l'utilisateur connecté. Pour en savoir plus sur l'authentification multifacteur, reportez-vous à la section Authentification multifacteur.
Actifs	Case à cocher indiquant si l'utilisateur connecté est actif ou inactif.
Agent d'utilisateur	Type de navigateur et système d'exploitation de l'appareil pour la session de connexion de l'utilisateur.
Adresse IP	Adresse IP de l'utilisateur connecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Dernier accès	Date et heure du dernier accès de cette session utilisateur à l'instance. **Remarque :** Pour afficher des informations détaillées sur une session de connexion particulière ou pour verrouiller la session elle-même, sélectionnez les champs **Agent utilisateur**, **Adresse IP** ou **Dernier accès** .

Mesures

Affichez les détails des types de mesures suivants :

Type de mesure	Description
Utilisateur	Mesures de sécurité associées à l'activité de l'utilisateur dans l'instance. Pour ouvrir la page Mesures utilisateur, sélectionnez le lien **Mesures** , puis Mesures **utilisateur**.
Exporter	Mesures de sécurité associées aux données exportées à partir de l'instance. Pour accéder à la page Mesures d'exportation, sélectionnez le lien **Mesures** , puis **Exporter les mesures**.
Authentification	Mesures de sécurité associées à l'authentification, telles que les adresses IP rarement utilisées, les échecs de connexion et les types de schémas d'authentification utilisés par vos utilisateurs. Pour accéder à la page Mesures d'exportation, sélectionnez le lien **Mesures** , puis Mesures **d'authentification**.
E-mail	Mesures de sécurité associées aux comportements anormaux liés aux e-mails entrants vers votre instance. Pour accéder à la page Mesures d'e-mail, sélectionnez le lien **Mesures**, puis sélectionnez **Mesures d'e-mail.**
Antivirus	Mesures de sécurité associées à l'activité de l'événement antivirus dans l'instance. Pour accéder à la page Mesures antivirus, sélectionnez la vignette **Antivirus** ou sélectionnez le lien **Mesures** , puis sélectionnez **Antivirus**.

Remarque :
Pour en savoir plus sur la surveillance de chaque type de mesure, consultez Surveiller les mesures d'instance.

Ressources

Accédez à Now Support Base de connaissances des articles, des ressources et des blogs liés à la sécurité des instances. Ces ressources incluent les paramètres de sécurité, le codage, la conformité, les correctifs et des sujets connexes. Pour accéder à la page Ressources :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Cliquez sur la vignette ou le lien **Ressources** .
2. Sur la page Ressources, sélectionnez une catégorie :

Catégorie	Description
Directives recommandées	Accès aux directives de sécurité recommandées, y compris les articles du Paramètres de sécurisation renforcéeGuide de codage sécurisé [KB0623354].
Ressources de sécurité	Accès aux ressources liées à la sécurité dans le Base de connaissances, notamment : ○ Test de sécurité de l'instance client ○ Articles de la base de connaissances du Centre de sécurité, de confiance et de conformité dans le cloud

Notifications de sécurité

Une icône de notifications en forme de cloche () apparaît dans Centre de sécurité de l'instance, avec un nombre total de notifications de sécurité non lues. Les notifications sont conservées et incluses dans ce décompte jusqu'à ce que vous les marquiez comme lues.

1. Cliquez sur l'icône en forme de cloche pour afficher les cinq premières notifications de sécurité non lues.

   Une notification s'affiche lorsque des événements **Connexion administrateur**, **Déverrouillage** administrateur, **Échec de la connexion**, **Rôle de privilège élevé**, **Emprunt d'identité**, **Élévation de la sécurité** et **Synthèse hebdomadaire** ont lieu dans votre instance. Pour en savoir plus sur ces événements de sécurité, reportez-vous à la section Surveiller les événements de sécurité.

2. Pour afficher des informations détaillées sur un événement de sécurité spécifique, sélectionnez la notification.

   Par exemple, si vous sélectionnez une notification de rôle de privilège élevé, vous pouvez afficher la table Rôles (sys_user_role). Cette table permet de déterminer quels utilisateurs ont reçu des rôles privilégiés au cours de la journée calendaire. L'utilisation de cet historique vous aide à déterminer si les rôles ont été correctement affectés.

3. S'il existe plus de cinq notifications non lues, sélectionnez **Afficher toutes les notifications** pour accéder à une page Toutes les notifications contenant une liste de toutes les notifications non lues.
   - Pour afficher des informations détaillées sur un événement de sécurité spécifique, sélectionnez la notification.
   - Pour marquer toutes les notifications répertoriées comme lues, sélectionnez **Marquer tout comme lu.**

Remarque :
En tant qu'administrateur, vous pouvez également configurer les préférences d'envoi de types spécifiques de notifications pour chaque type d'événement de sécurité. Pour en savoir plus, consultez Définir les préférences pour les notifications d'événements de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visites guidées

Cliquez sur le lien **Visites guidées** pour afficher une visite visuelle guidée du Centre de sécurité de l'instance.

- La visite guidée comprend uniquement les fonctions de surveillance de sécurité répertoriées sur la page d'accueil.
- Elle n'inclut pas les fonctions de sécurité auxquelles vous accédez lorsque vous sélectionnez les tuiles ou les liens de la page d'accueil.

Portail de test de sécurité, centre de sécurité et aide

Il s'agit Now Support Portail de services d'une ressource centrale que vous utilisez pour gérer les instances, les tâches et les comptes. Vous pouvez également accéder à des ressources utiles pour diagnostiquer et résoudre les problèmes techniques et de sécurité dans votre instance.

Pour accéder à ces ressources, sélectionnez **En savoir plus** ou Obtenez de l'aide dans les tuiles suivantes :

Mosaïque	Description
Portail de test de la sécurité	Accès au tableau de bord de la sécurité dans le portail de Now Support test de sécurité.
Centre de sécurité	Accès à la conformité de sécurité dans le Now Support portail de sécurité.

Aide	Accès aux ressources d'aide suivantes dans le portail de Now Support sécurité :
	• Demandez à un expert de trouver des réponses aux questions courantes.
	• Signalez un problème ou une panne à l'assistance ServiceNow technique globale en ouvrant un ticket.
	• Ressources d'assistance en libre-service, notamment :
	  ◦ Vidéos
	  ◦ Documentation
	  ◦ ServiceNow Community
	  ◦ Base de connaissances
	  ◦ Portail d'erreurs connues
	  ◦ Base de données RFX de sécurité
	• ServiceNow Community Questions recommandées pour votre utilisation.

Accès à Agent virtuel

Il s'agit Agent virtuel d'une plate-forme permettant de fournir une assistance aux utilisateurs par le biais de conversations au sein d'une interface de messagerie.

Une fois les modules d'extension associés installés, les administrateurs peuvent accéder aux Agent virtuel fonctions et Compréhension du langage naturel (NLU) en sélectionnant l'icône Agent virtuel :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il vous permet d'effectuer les tâches suivantes :

- Posez des questions liées à la sécurité, puis obtenez des réponses récapitulatives rapides et des liens de référence pour en savoir plus.
- Obtenez des réponses liées aux processus tels que :
  - Centre de sécurité de l'instance
  - Sécurité de la plateforme
  - ServiceNow Politiques de sécurité
  - Confiance, gouvernance et risque
- Recherchez des ressources liées à la sécurité, telles que Base de connaissances des rubriques dans le Now Support portail de sécurité.

Remarque :
Pour en savoir plus sur l'utilisation et l'activation de , Agent virtuel consultez :

- Agent virtuel
- Activer l'interface ISC Agent virtuel

Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration

Découvrez les principales différences lors de la migration du Centre de sécurité de l'instance (ISC) vers ServiceNow Centre de sécurité (SSC).

Important :

Instance Security Center est un produit hérité qui atteindra la fin de la commercialisation d'ici septembre 2024. ServiceNow Security Center est la solution que les clients recommandent d'adopter à l'avenir. Pour plus d'informations, consultez l'article sur le processus de dépréciation (KB0867184) dans la base de connaissances Now Support.

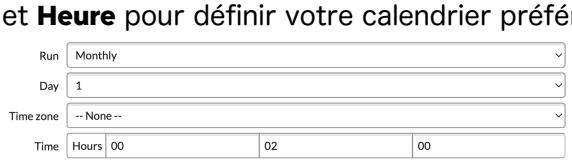
ServiceNow Centre de sécurité (SSC) est une application de sécurité qui consiste en un ensemble d'outils spécialement conçus pour aider les organisations à maintenir la sécurité de leurs ServiceNow déploiements. Grâce à SPC, les organisations peuvent améliorer leur posture de sécurité, renforcer leurs niveaux de conformité et le faire avec une expérience utilisateur transparente.

Utilisez ce document pour en savoir plus sur les améliorations apportées aux fonctionnalités de SPC et sur la façon d'exécuter des tâches qui étaient auparavant effectuées dans SPC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurisation renforcée de la sécurité

Améliorations des fonctionnalités	ISC contre SSC
Mises à jour des interactions de l'utilisateur	• Examinez le dernier score en accédant à la page Vue d'ensemble ou comparaison de la sécurisation renforcée. • Mettez à jour manuellement le dernier score en accédant à Vue d'ensemble et en sélectionnant Mettre à jour le score. • Modifiez la configuration des paramètres en sélectionnant un lien de nom de paramètre sur l'une de ces pages, puis apportez des modifications sur la page **détaillée Paramètres** : ○ Vue d'ensemble ○ **Sécurisation renforcée** > **Tous les paramètres** ○ **Sécurisation renforcée** > **Comparaison**
Définir un calendrier pour recalculer votre score de conformité	À l'aide de SSC, vous pouvez définir quand le système déclenche une actualisation de votre score de conformité. **1.** Accédez à la table Exécutions de script planifiées [sysauto_script]. **2.** Recherchez et ouvrez l'enregistrement SC - Calculer la conformité mensuelle . **3.** Utilisez les champs **Exécuter**, **Jour**, **Fuseau horaire** et **Heure** pour définir votre calendrier préféré.  **4.** Sélectionnez **Mettre à jour** pour enregistrer vos changements.

KPI et mesures de sécurité

Améliorations des fonctionnalités	ISC contre SSC
Améliorations apportées aux KPI	À l'aide de SSC, vous pouvez : • Affichez la tendance du score dans le temps. • Surveillez tous les KPI et mesures à l'aide de la même interface et des mêmes options d'analyse.
Améliorations apportées aux mesures	SPC comprend les améliorations suivantes aux mesures :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Améliorations des fonctionnalités	ISC contre SSC
	• Plus de 65 mesures ont été ajoutées. • Surveillez et analysez les KPI et les mesures à partir d'une interface utilisateur unique. • Créez des cibles et des seuils pour les mesures.
Mises à jour des interactions de l'utilisateur	Accéder aux mesures dans SSC en accédant à **Vue d'ensemble** > **Mesures**, puis en sélectionnant la mesure dans le menu de navigation. Vous pouvez également accéder à **Toutes les mesures**.

Scanner de sécurité

Améliorations des fonctionnalités	ISC contre SSC
Nouvelle fonctionnalité	SPC comprend les fonctions suivantes : • Exécuter manuellement des analyses ou les planifier pour qu'elles s'exécutent à des moments spécifiques. • Créez vos propres vérifications d'analyse. • Créez votre propre suite d'analyse. • Comparez les résultats de deux analyses.
Fonctionnalité d'e-mail améliorée	Configurez des notifications par e-mail pour rester informé des événements de sécurité sur votre instance.
Mises à jour des interactions de l'utilisateur	• Exécutez l'analyse de l'auditeur en accédant à **Vue d'ensemble** > **Analyse** > **Suites** et en sélectionnant **Auditor Suite** dans la liste. • Afficher les résultats de l'analyse en accédant à **Vue d'ensemble** > **Analyse** > **Résultats**.

Fonctionnalités de sécurité supplémentaires

Améliorations des fonctionnalités	ISC contre SSC
Surveiller la fonctionnalité des sessions	• Visualisez les activités de session à l'aide du Analytics Hub fichier . • Surveillez l'activité de la session en accédant à **Mesures** > **Sessions**.
Trouver des ressources	Accédez à toutes les ressources d'apprentissage sur une seule page à l'adresse **Vue d'ensemble** > **Apprentissage**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se désabonner des Centre de sécurité fonctionnalités

Pour désactiver Centre de sécurité des fonctionnalités sur votre instance, suivez les étapes indiquées dans KB1702514 : Directives pour désactiver les composants du Centre de sécurité de l'instance (lors de l'utilisation du Centre de sécurité).

Surveiller les événements de sécurité

Analysez les mesures d'événements dans votre instance afin de pouvoir identifier et prévenir les événements de sécurité potentiels.

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

Dans le ruban d'événement, qui se trouve sur la page d'accueil Sécurité de l'instance, vous pouvez analyser ces mesures et les détails qui les accompagnent pour identifier les événements de sécurité potentiels dans l'instance.

- Pour chaque mesure d'événement, un score unique en temps réel s'affiche, indiquant combien de fois l'événement s'est produit au cours de la journée dans cette instance. Ces rapports à score unique sont mis à jour automatiquement au fur et à mesure que les événements correspondants se produisent.
- Chaque mesure d'événement contient également des informations de conformité, des tendances et des graphiques sur une plage de dates. Ces informations sont mises à jour quotidiennement lorsque vous exécutez la tâche d'analyse des performances. Pour en savoir plus, reportez-vous à la section **de détail Analyse de la tendance des événements** .

Types d'événements

Vous pouvez surveiller au moins six des types d'événements suivants. Pour plus de six événements, utilisez les flèches gauche ou droite sous le ruban d'événement pour les faire défiler. Pour plus d'informations sur la configuration du ruban d'événement, reportez-vous à la section Configurer le ruban d'événement de sécurité.

Préférence de notification	Description
Connexions des administrateurs	Nombre de tentatives de connexion dans cette instance, au cours de la journée calendaire, par les utilisateurs à qui un rôle administrateur a été affecté.
Utilisateurs administrateurs ajoutés	Nombre d'utilisateurs dotés d'un rôle administrateur qui ont été ajoutés dans cette instance au cours de la journée calendaire. Par exemple, votre instance peut rencontrer un problème de sécurité si le nombre est de 10, mais que 4 utilisateurs sont connus pour avoir un rôle administrateur affecté.
E-mail entrant externe	Pour en savoir plus, consultez Mesures d'e-mail.
Connexions externes	Nombre d'utilisateurs avec un rôle de snc_external affecté qui se sont connectés à cette instance au cours de la journée calendaire. Ces connexions ont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférence de notification	Description
	généralement lieu à des fins de maintenance, de support, de conseil ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et non des problèmes de sécurité potentiels. Pour en savoir plus sur l'affectation de rôles d'utilisateur externes, reportez-vous à la section Explicit Roles.
Échecs de connexion	Nombre de tentatives de connexion qui ont échoué dans cette instance au cours de la journée calendaire. Cette mesure peut indiquer que des tentatives de connexion sont effectuées et compromettent la sécurité de votre instance.
Emprunts d'identité	Nombre de connexions par emprunt d'identité dans cette instance au cours de la journée calendaire. Pour en savoir plus sur l'emprunt d'identité des utilisateurs, consultez la rubrique Emprunter l'identité d'un utilisateur .
Fichiers en quarantaine	Nombre de fichiers qui ont été mis en quarantaine lors de l'exécution Analyse antivirus dans cette instance au cours de la journée calendaire. Pour en savoir plus sur les fichiers mis en quarantaine et Analyse antivirus, reportez-vous à la section Mesures antivirus et Analyse antivirus.
Élévations de la sécurité	Nombre de fois qu'un administrateur de sécurité a élevé la sécurité pour les utilisateurs standard en changeant le rôle d'utilisateur qui leur est affecté en un rôle de sécurité avec privilège élevé au cours de la journée calendaire. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, administrateur, security_admin et emprunteur d'identité. • Cette mesure indique que quelqu'un a peut-être essayé d'élever la sécurité d'un utilisateur non autorisé. N'utilisez pas cette mesure seule pour détecter une compromission de sécurité spécifique. Traitez plutôt cette mesure comme une indication que vous devez vérifier une autre mesure pour voir si une compromission de sécurité s'est produite. • Pour en savoir plus sur l'amélioration de la sécurité des utilisateurs, reportez-vous aux sections Accéder à un rôle privilégié et Rôles à privilèges élevés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférence de notification	Description
Connexions SNC	Nombre de personnes qui se sont connectées à cette instance à l'aide de Service client et assistance la technique hi-hopping au cours de la journée calendaire. Ces connexions ont généralement lieu à des fins de maintenance, de support, de conseil ou d'audit. Pour plus d'informations sur le contrôle de l'accès ServiceNow des employés de l'entreprise, consultez Contrôle d'accès ServiceNow.
Courrier indésirable	Pour en savoir plus, consultez Mesures d'e-mail.
E-mail entrant approuvé	Pour en savoir plus, consultez Mesures d'e-mail.
E-mail entrant non approuvé	Pour en savoir plus, consultez Mesures d'e-mail.
Types de virus	Nombre de types différents d'événements antivirus qui se sont produits dans cette instance au cours de la journée calendaire. Pour en savoir plus sur les types d'événements antivirus, consultez Mesures antivirus.

Analyse du détail de la tendance de l'événement

Pour afficher les détails de tendance d'une mesure d'événement, cliquez sur le nombre d'événements pour accéder à la page du centre d'analyse. Les détails qui s'affichent pour l'instance dépendent du type de mesure.

Par exemple, pour afficher la liste de chaque tentative infructueuse sur la page Journaux des événements du tableau de bord de sécurité :

- Sélectionnez la mesure **Échecs de connexion** .
- Dans la page, cliquez sur Afficher les Centre d'analyse**enregistrements**.
- Cliquez sur l'une des tentatives de connexion infructueuses.
- Le détail comprend le nom de l'utilisateur qui a tenté de se connecter, son adresse IP et le nom de la table à laquelle il a essayé d'accéder.

Vous pouvez configurer des déclencheurs de seuil d'événement dans le Interface utilisateur principale Centre d'analyse ou Platform Analytics Détails des KPI pour fournir des alertes lorsqu'un certain événement se produit dans une plage de scores pour un *indicateur*. Vous pouvez également définir des cibles qui vous permettent de visualiser la différence entre le score souhaité et le score réel d'un événement.

Par exemple, vous pouvez définir un seuil de 10 pour la mesure **Échecs de connexion** . Lorsque dix tentatives de connexion ou plus échouent au cours de la journée, une alerte est envoyée à un personnel de sécurité spécifique. Vous pouvez également définir une cible similaire qui fournit une mise en évidence visuelle lorsque Centre d'analyse 10 échecs de connexion se produisent au cours d'une journée.

Les données et graphiques de tendance qui s'affichent dans la tuile du ruban d'événement et qui sont mis à jour après l'exécution Centre d'analyse de la tâche d'analyse des performances à 2h00, heure locale. Pour en savoir plus, consultez Actualisation quotidienne des données de score, de tendance et de graphique de conformité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Centre de sécurité de l'instance

Now Intelligence

Centre d'analyse

Cibles et seuils d'Analyse des performances

Configurer le ruban d'événement de sécurité

Configurez le ruban d'événement de sécurité sur la page d'accueil du Centre de sécurité de l'instance pour inclure uniquement les événements pertinents pour le suivi de la sécurité d'instance dans vos opérations. Vous pouvez également modifier l'ordre dans lequel les tuiles d'événement de sécurité apparaissent sur le ruban.

Avant de commencer

Rôle requis : security_dashboard_user ou admin

Pourquoi et quand exécuter cette tâche

Le ruban d'événement de sécurité est initialement renseigné avec un ensemble complet d'événements de sécurité standard. Vous pouvez la personnaliser en supprimant les événements qui ne sont pas pertinents pour votre organisation.

- Par exemple, si vous pensez que les problèmes de sécurité sont dus aux actions du personnel interne, incluez les indicateurs d'événements Connexions d'administrateur, Utilisateurs administrateurs ajoutés et Élévations de sécurité.
- Ces indicateurs surveillent le nombre de fois où des utilisateurs ayant des rôles d'administrateur ont tenté de se connecter et, si des utilisateurs administrateurs ont été ajoutés, quelles tentatives ont été faites pour élever les rôles de sécurité.

Remarque :
Pour en savoir plus sur les types d'événements de sécurité qui apparaissent dans le ruban d'événement, reportez-vous à la section Surveiller les événements de sécurité.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Dans le ruban de l'événement, cliquez sur **Modifier** (< > Edit).
   Dans le formulaire Modifier les événements, la colonne **Sélectionné** contient les événements déjà répertoriés.
3. Pour ajouter des événements de sécurité au ruban d'événement, déplacez-les de la colonne **Disponible** vers la colonne **Sélectionné** .
   Pour modifier l'ordre d'apparition des événements sur le ruban, sélectionnez un événement, puis cliquez sur la flèche vers le haut ou vers le bas pour le déplacer vers sa position correcte.
   - Placez les événements dans le même ordre séquentiel qu'ils doivent apparaître sur le ruban d'événement du Centre de sécurité de l'instance.
   - Les événements que vous placez en haut de la colonne **Disponible** apparaissent séquentiellement, en commençant sur le côté gauche du ruban d'événement Centre de sécurité de l'instance. Les événements placés vers le bas de la colonne apparaissent à droite sur le ruban de l'événement.
4. Pour supprimer les événements de sécurité du ruban d'événement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans la colonne **Sélectionné** , sélectionnez les événements de sécurité que vous souhaitez supprimer du ruban de l'événement.
- Déplacez-les de la colonne **Sélectionné** vers la colonne **Disponible** .

5. Cliquez sur **Enregistrer**.

Information associée

Centre de sécurité de l'instance

Définir les préférences pour les notifications d'événements de sécurité

Configurez les préférences pour les types de notifications que vous souhaitez recevoir pour les occurrences d'événements de sécurité spécifiques. Pour chaque type, vous indiquez si vous souhaitez recevoir des notifications par e-mail, par notification push dans Now Mobile ou dans des applications de messagerie tierces telles que Slack ou Microsoft Teams.

Avant de commencer

Pour permettre aux applications de messagerie tierces d'envoyer des notifications d'événements de sécurité, vous devez activer le module d'extension Messaging Notification (com.glide.notification.messaging). Les utilisateurs individuels doivent configurer leurs propres paramètres. Pour plus d'informations, voir Notifications dans les applications de messagerie .

Rôle requis : admin.

Procédure

1. Sur la page d'accueil du Centre de sécurité de l'instance, cliquez sur le menu de profil, puis sur **Préférences de notification**.

Préférences de notification

Préférence de notification	Description
Connexion de l'administrateur	Envoyez le type sélectionné de notification chaque fois que d'autres utilisateurs avec des rôles d'administrateur affectés se connectent à cette instance à partir d'une adresse IP différente.
Déverrouillage administrateur	Envoyez le type sélectionné de notification chaque fois qu'un compte d'utilisateur aux privilèges élevés a été déverrouillé.
Échec de la connexion	Envoyer le type sélectionné de notification chaque fois que d'autres utilisateurs ne parviennent pas à se connecter à cette instance en moins de tentatives que le nombre défini dans la `glide.user.max_unlock_attempts` propriété. Si vous ne configurez pas cette propriété, la valeur par défaut est 5. Pour en savoir plus sur cette propriété, reportez-vous à la section Spécifier le verrouillage en cas d'échec des tentatives de connexion.
Rôle HP ajouté	Envoyez le type de notification sélectionné chaque fois qu'un rôle de sécurité de privilège élevé (y

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférence de notification	Description
	compris les rôles oauth_admin, administrateur, security_admin et emprunteur d'identité) est accordé à un autre utilisateur. Pour en savoir plus sur l'amélioration de la sécurité des utilisateurs, reportez-vous aux sections Accéder à un rôle privilégié et Rôles à privilèges élevés.
Emprunt d'identité	Envoyez le type sélectionné de notification chaque fois qu'un autre utilisateur emprunte votre identité. Pour en savoir plus sur l'emprunt d'identité d'un utilisateur, consultez la rubrique Emprunter l'identité d'un utilisateur .
Élévation de la sécurité	Envoyez le type sélectionné de notification chaque fois que d'autres utilisateurs sont élevés au rôle d'administrateur de sécurité dans cette instance.
Synthèse hebdomadaire	Envoyer une synthèse hebdomadaire sur le type de notification sélectionné. Inclut : ○ Résumé de toutes les activités de sécurité qui ont eu lieu dans cette instance tout au long de la semaine. ○ Score de conformité quotidien actuel de l'instance.

2. Pour chaque type d'événement de sécurité, cochez les cases appropriées afin de désigner le type de notifications à vous envoyer.
   Vous pouvez sélectionner plusieurs méthodes de notification pour chacun.

3. Cliquez sur **Enregistrer**.

Vérifier le score de conformité quotidien et configurer les paramètres des propriétés de sécurité

Examinez la mesure du score de conformité quotidien et les propriétés de configuration de sécurité pour voir si votre instance est conforme aux exigences de sécurité suggérées. Vous pouvez affecter le score de conformité quotidien en mettant à jour les propriétés de sécurité non conformes dans la page Configurations de la conformité à la sécurisation renforcée.

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le score de conformité quotidien est un score en pourcentage. Elle est basée sur le degré de conformité des paramètres actuels de vos propriétés de sécurité d'instance avec les valeurs de conformité publiées dans le Paramètres de sécurisation renforcée.

Vérifiez régulièrement le score de conformité quotidien de votre instance. Suivez ces instructions lorsque vous évaluez votre score de conformité quotidien :

- Une valeur supérieure ou égale à 90 % indique que l'instance est conforme aux contrôles de sécurité critiques.
- Une valeur supérieure ou égale à 50 % et inférieure à 90 % indique un niveau modéré de conformité de la sécurité.
- Moins de 50 % indique un faible niveau de conformité de la sécurité.

Ajuster les paramètres de sécurité de l'instance pour accroître la conformité

À l'aide de la page Configuration de la conformité à la sécurisation renforcée, renforcez et optimisez les propriétés de sécurité non conformes qui affectent le score de conformité quotidien de votre instance. Son utilisation garantit que votre instance est conforme aux normes de renforcement de la sécurité publiées, tout en répondant aux exigences de sécurité de votre entreprise.

Avant de commencer

Rôle requis : security_dashboard_user ou administrateur.

Consultez le contenu pour obtenir Paramètres de sécurisation renforcée des descriptions détaillées et les valeurs de conformité des propriétés système et des modules d'extension liés à la sécurité dans le ServiceNow AI Platform.

- Consultez les paramètres de renforcement de la sécurité de l'instance chaque fois que vous définissez ou mettez à jour des propriétés liées à la sécurité, même si certaines des valeurs de conformité peuvent ne pas convenir à votre instance.
- Lorsque vous mettez à jour ces propriétés, assurez-vous que l'instance continue de se comporter comme prévu. Consultez le personnel interne approprié qui possède l'expertise nécessaire pour déterminer les impacts sur la sécurité.

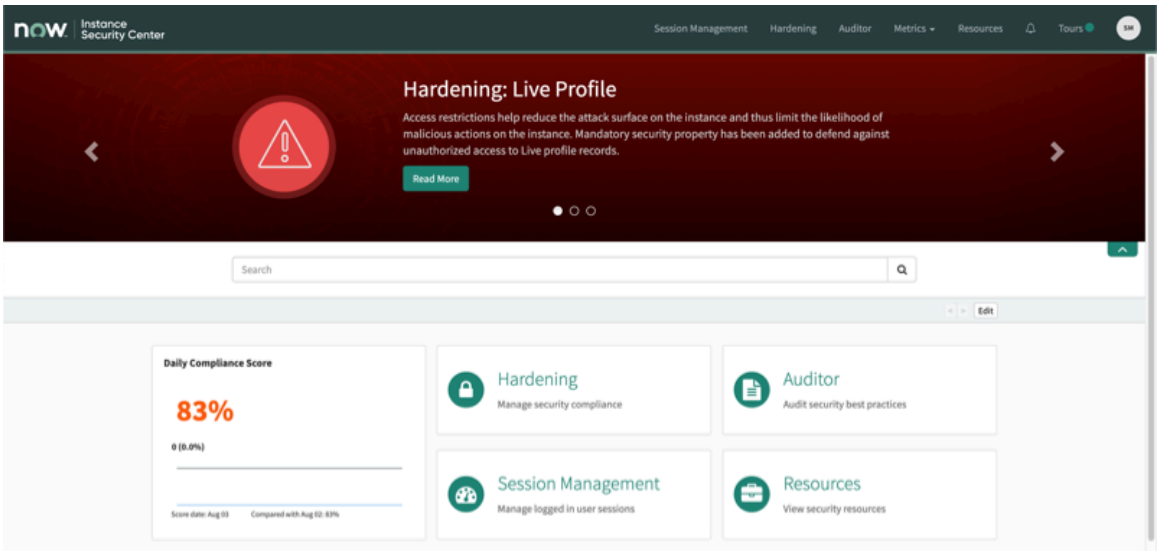
Remarque :
Si vous disposez d'un rôle administrateur, vous pouvez afficher et modifier les contrôles de sécurité. Si vous disposez d'un rôle security_dashboard_user, vous pouvez afficher les contrôles de sécurité, mais vous ne pouvez pas les modifier.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Cliquez sur la vignette du **score de conformité quotidienne** ou sur le lien de **sécurisation renforcée** pour accéder à la page de configuration de la conformité à la sécurisation renforcée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

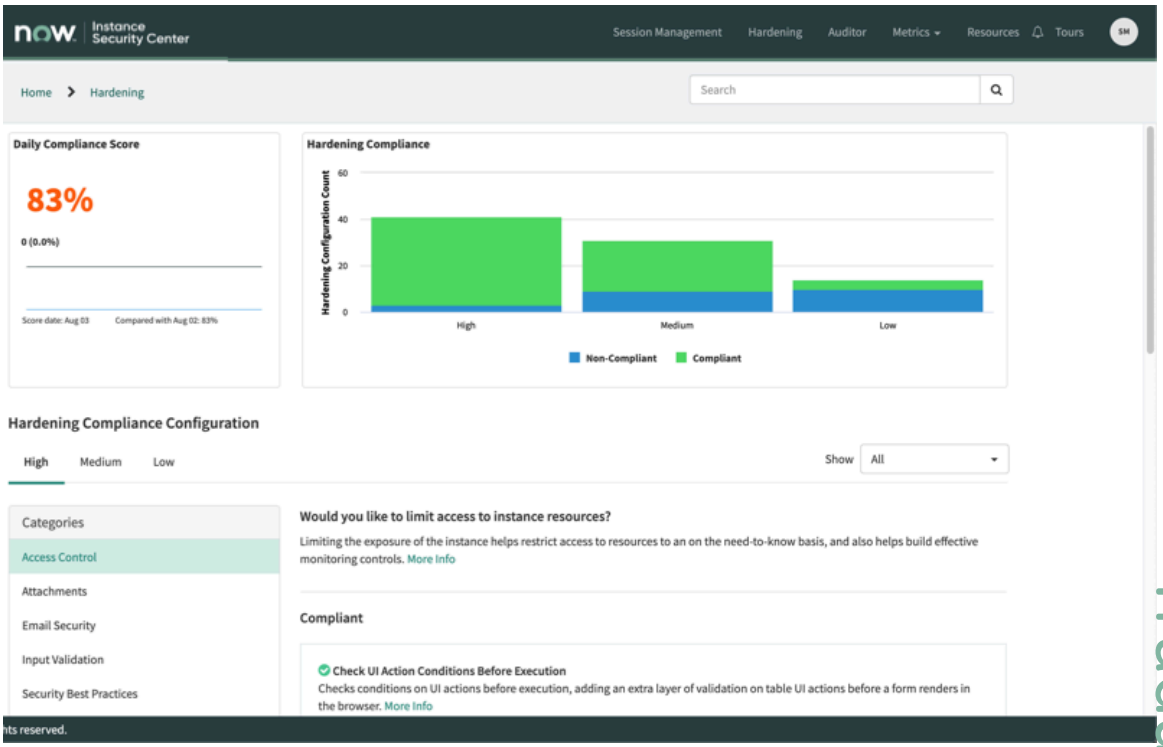


3. Dans le graphique Conformité à la sécurisation renforcée, affichez les statistiques relatives aux propriétés de configuration de sécurité conformes et non conformes.

Option	Description
Conforme	Nombre de propriétés de configuration de sécurité conformes aux valeurs de conformité indiquées dans les paramètres de renforcement de la sécurité de l'instance. **Remarque :** Vous ne pouvez pas modifier les paramètres des propriétés de sécurité conformes dans la configuration de la conformité à la sécurisation renforcée. Si vous le souhaitez, vous devez les mettre à jour dans les propriétés système. Pour en savoir plus, consultez Ajouter une propriété système .
Non conforme	Nombre de propriétés de configuration de sécurité qui ne sont pas conformes aux valeurs de conformité dans les paramètres de renforcement de la sécurité de l'instance. Vous pouvez mettre à jour les paramètres des propriétés non conformes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



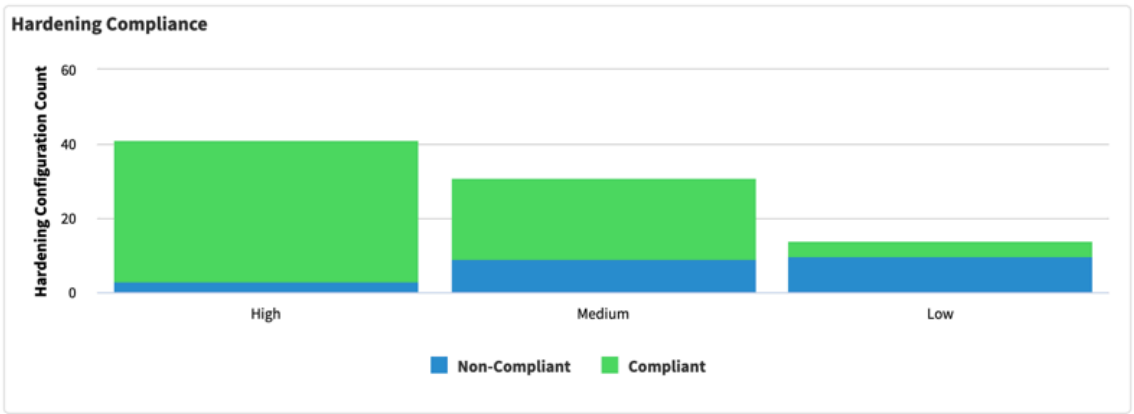
Remarque :
Pour afficher le nombre de scores de sécurité conformes ou non conformes sur une plage de dates, déplacez le point bleu sur le curseur sous le score de conformité quotidien.

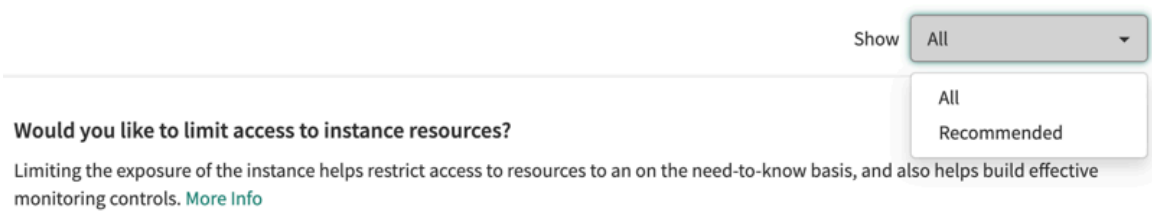
4. Dans la liste **Afficher** sous le graphique, indiquez si vous souhaitez accéder à toutes les propriétés de configuration de sécurité ou uniquement à celles qui sont recommandées.

Option	Description
Tous	(Par défaut) Toutes les propriétés de configuration de sécurité conformes et non conformes dans chaque catégorie sélectionnée.
Recommandé	Seules les propriétés de configuration de sécurité recommandées apparaissent dans chaque catégorie sélectionnée. Ces propriétés de configuration de sécurité sont un sous-ensemble sélectionné des propriétés les plus critiques utilisées pour sécuriser le ServiceNow AI Platform. Considérez ces propriétés de configuration de sécurité comme le nombre minimal de paramètres que vous devez définir pour sécuriser le ServiceNow AI Platform. **Remarque :** Pour sécuriser entièrement votre instance, utilisez l'option **Tout** . Elle inclut également toutes les propriétés de configuration de sécurité recommandées.

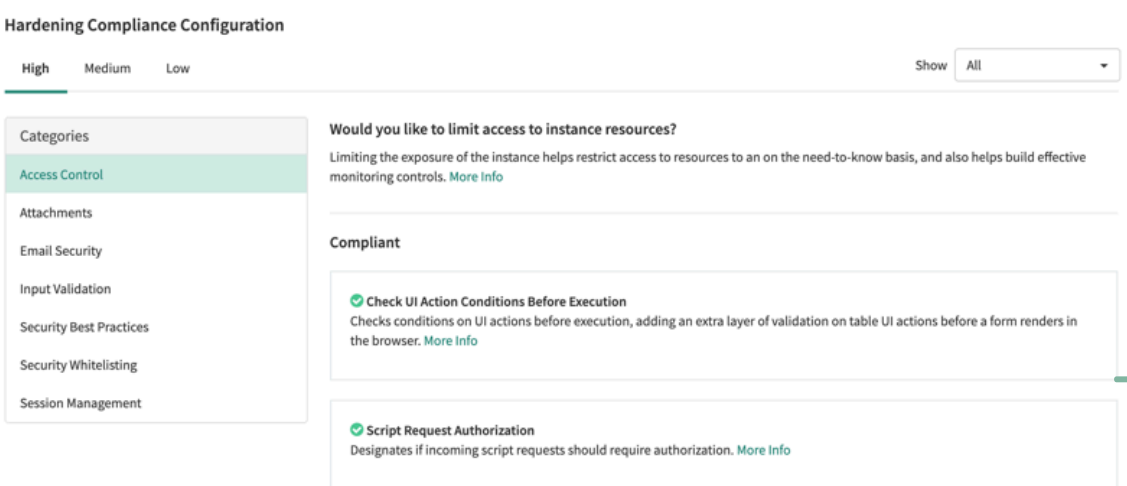
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





5. Dans **Catégories**, sélectionnez la catégorie qui contient les propriétés de configuration de sécurité auxquelles vous souhaitez accéder :



Option	Description
Contrôle d'accès	Les contrôles d'accès déterminent s'il faut accorder ou refuser l'accès des utilisateurs à une ressource particulière en fonction des personnes autorisées à utiliser ces ressources. Pour en savoir plus, consultez Contrôle d'accès les paramètres de renforcement de la sécurité de l'instance.
Pièces jointes	Les contrôles de sécurité des pièces jointes permettent de valider les pièces jointes entrantes afin de protéger votre instance contre les fichiers malveillants envoyés par des attaquants. Pour en savoir plus, consultez Valider le type MIME de fichier dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	AttachmentCreator SOAP Web Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5] les paramètres de renforcement de la sécurité de l'instance.
Sécurité de la messagerie	La sécurité de la messagerie englobe des propriétés de configuration de sécurité qu'un administrateur peut configurer pour s'assurer que des politiques de sécurité appropriées sont en place pour tous les e-mails entrants. Pour en savoir plus, consultez Activer la notation et le filtrage d'e-mail indésirable [Mis à jour dans Centre de sécurité 1.3] les paramètres de renforcement de la sécurité de l'instance.
Validation de l'entrée	La validation d'entrée comprend des propriétés liées à la sécurité qu'un administrateur peut configurer pour minimiser la saisie de données mal formées, quelle que soit la source. Pour en savoir plus, consultez Validation, nettoyage et codage les paramètres de renforcement de la sécurité de l'instance.
Communications sécurisées	Les propriétés de communications sécurisées sont celles qu'un administrateur peut configurer pour sécuriser le transport du trafic HTTP. Pour en savoir plus, consultez Communications les paramètres de renforcement de la sécurité de l'instance.
Bonnes pratiques de sécurité	Les bonnes pratiques de sécurité englobent les tâches de sécurité qu'un administrateur doit effectuer périodiquement, dans un certain intervalle de temps, ainsi que les propriétés de configuration connexes. Pour en savoir plus, consultez Bonnes pratiques de sécurité les paramètres de renforcement de la sécurité de l'instance.
Liste d'inclusion de sécurité	La liste d'inclusion de sécurité comprend des propriétés liées à la sécurité qu'un administrateur peut configurer pour restreindre le comportement aux listes d'inclusion connues.
Gestion des sessions	La gestion des sessions inclut des propriétés liées à la sécurité qu'un administrateur peut configurer pour garantir une gestion sécurisée des sessions dans le ServiceNow AI Platform. Pour en savoir plus, consultez Gestion des sessions les paramètres de renforcement de la sécurité de l'instance

6. Configurez les propriétés de sécurité non conformes dans la catégorie sélectionnée.
   - Sauf indication contraire, le fait de faire glisser le commutateur définit une propriété de sécurité sur le paramètre recommandé. Par exemple, vous définissez la plupart des contrôles sur vrai ou faux, mais certains nécessitent la saisie d'une ou de plusieurs valeurs, telles qu'une liste de valeurs séparées par des virgules.
   - Pour accéder à la rubrique Paramètres de la sécurisation renforcée de la sécurité de l'instance dédiée au contrôle de sécurité et en savoir plus à son sujet, cliquez sur **Plus d'informations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Le score de conformité quotidienne augmente ou diminue en fonction des changements que vous apportez aux paramètres des contrôles de sécurité non conformes.

Information associée

Centre de sécurité de l'instance

Actualisation quotidienne des données de score, de tendance et de graphique de conformité

Les données de tendance et de graphique dans Centre de sécurité de l'instance sont mises à jour après l'exécution de la tâche d'analyse des performances à 02h00, heure locale. Il apparaît dans la tuile Score de conformité quotidien, dans les tuiles du ruban Événement et dans le détail de la Centre d'analyse page lorsque vous cliquez sur l'une des tuiles d'événement.

La tâche de gestion quotidienne des données [AppSec] est une tâche planifiée régulière qui s'exécute tous les soirs et effectue les tâches suivantes :

1. Vérifie si des utilisateurs valides ont été affectés aux travaux de gestion quotidienne des données [AppSec] et de collecte de données quotidiennes [PA AppSec] lorsque vous les planifiez pour la première fois.
   - Si vous avez saisi un utilisateur valide dans le champ **Exécuter en tant que** , le traitement de la tâche se poursuit. Un utilisateur valide est un utilisateur qui n'est pas verrouillé hors de l'instance et qui dispose d'un rôle administrateur affecté.
   - Si vous avez saisi un utilisateur non valide, un message d'erreur s'affiche au-dessus de la bannière de sécurité rotative dans le Centre de sécurité de l'instance.

   Remarque :
   Pour en savoir plus sur la mise à jour de l'utilisateur affecté lors de l'exécution de travaux planifiés, voir Créer ou planifier un travail de collecte de données .

2. Exécute la logique métier pour définir l'état de conformité pour les propriétés de sécurité que vous configurez dans la page Configuration de la conformité à la sécurisation renforcée. Pour en savoir plus, consultez Vérifier le score de conformité quotidien et configurer les paramètres des propriétés de sécurité.
3. Exécute la tâche d'analyse des performances de la collecte de données quotidienne [PA AppSec] pour collecter des données de conformité et mettre à jour le score de conformité quotidien.

Actualiser manuellement le score de conformité quotidien

Si vous disposez d'un rôle administrateur affecté, vous pouvez également actualiser et recalculer le score de conformité quotidien à tout moment en cliquant sur **Actualiser**.

Remarque :
Le bouton **Actualiser** n'apparaît pas pour les utilisateurs à qui un rôle de security_dashboard_user est affecté.

Traduction automatique

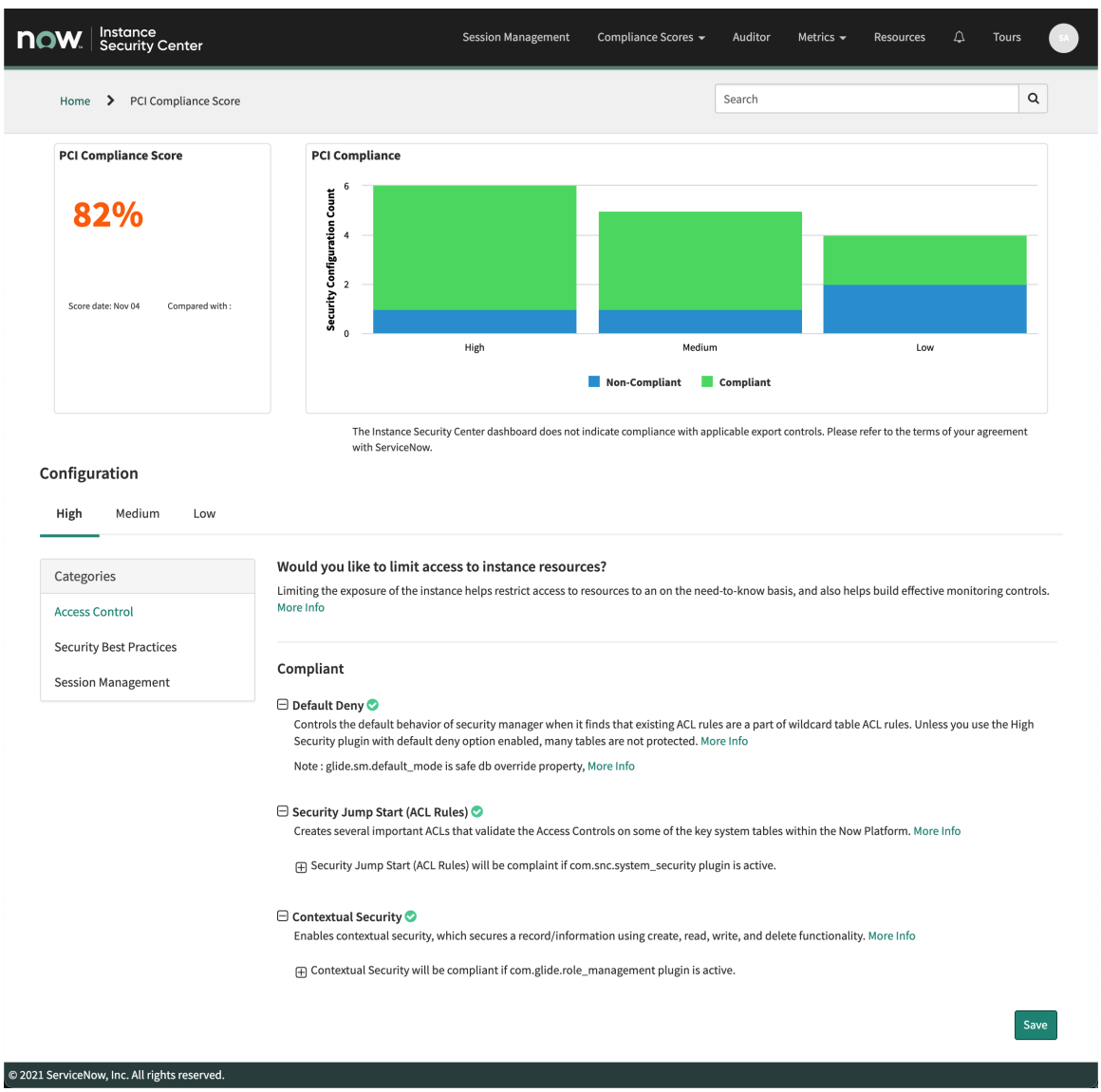
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La fonction d'actualisation effectue les mêmes tâches que la tâche d'analyse des performances de collecte de données quotidiennes, mais en temps réel plutôt que par lots.
- Vous l'utilisez généralement lorsque vous souhaitez effectuer des mises à jour du score de conformité quotidien pour visualiser immédiatement l'impact des activités de sécurité de l'instance.
- Il peut y avoir un léger délai avant que le score mis à jour n'apparaisse.

Remarque :
Lorsque vous effectuez une mise à niveau (par exemple, de àYokohama), le module d'extension Centre de London sécurité de l'instance (ISC) est automatiquement activé. Un script correctif fourni affecte automatiquement un utilisateur personnalisé sans aucun rôle affecté.

Tableau de bord des scores de conformité PCI

Le tableau de bord des scores de conformité PCI indique comment votre instance est conforme aux normes de sécurité du secteur des cartes de paiement (PCI). Utilisez le tableau de bord pour afficher votre score de conformité et modifiez votre configuration pour améliorer la sécurité.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles ServiceNow AI Platform requis

security_dashboard_user ou administrateur nécessaire pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des scores de conformité PCI

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l'instance, cliquez sur **Scores de conformité** dans l'en-tête, puis sélectionnez **Score de conformité PCI**.

Cas d'utilisation

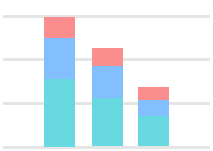
Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité de la sécurité des instances.
Admin (admin)	Surveillez en permanence la conformité de la sécurité de l'instance pour détecter les menaces de sécurité et y répondre.

Indicateurs

Indicateur	Description
Score de conformité PCI	Affiche le score de conformité de votre instance sous forme de pourcentage. Ce pourcentage représente le pourcentage de configurations de sécurité sur votre instance qui répondent aux normes de conformité. L'indicateur affiche également la date à laquelle le score de conformité a été calculé et une comparaison avec le score calculé précédent.

Visualisation des données

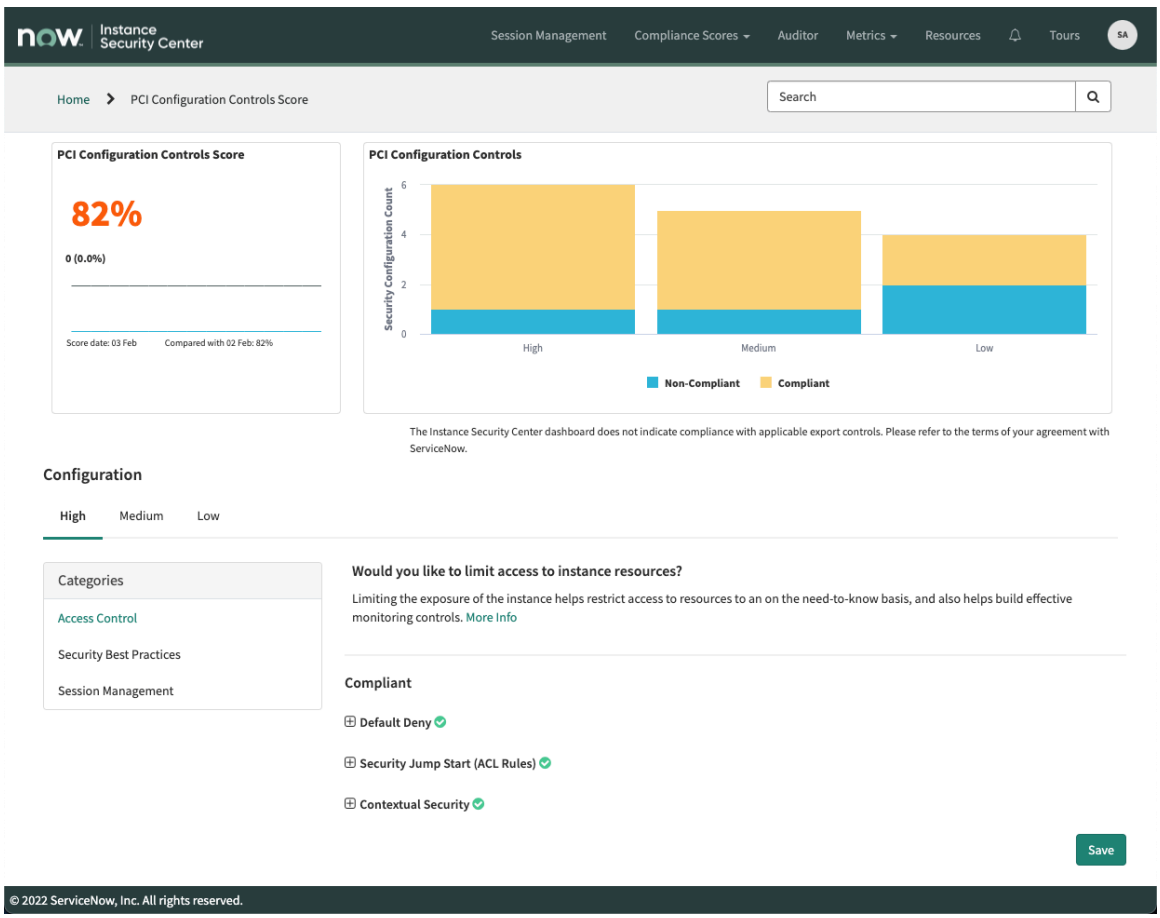
Titre	Type	Table source	Description
Conformité PCI	 Graphique à barres empilées	Configurations de sécurité [isc_security_configurations]	Affiche les configurations de sécurité conformes et non conformes dans les catégories élevée, moyenne et faible. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord des scores des contrôles des configurations PCI

Utilisez le tableau de bord des scores des contrôles de configuration PCI pour examiner votre configuration PCI et déterminer quels contrôles de sécurité ne sont pas conformes. Vous pouvez modifier la configuration des contrôles de sécurité non conformes à partir du centre de sécurité de l'instance.



Rôles ServiceNow AI Platform requis

Le rôle security_dashboard_user ou administrateur est requis pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des scores des contrôles de configuration PCI

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l'instance, cliquez sur **Scores de conformité** dans l'en-tête, puis sélectionnez **Score des contrôles des configurations PCI**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité des contrôles de configuration PCI sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

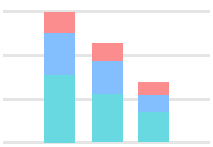
Utilisateur	Utilisation du tableau de bord
	Modifiez la configuration PCI pour garantir la conformité et améliorer la sécurité de l'instance.
Admin (admin)	Surveillez en permanence la conformité des contrôles de configuration PCI pour détecter et répondre aux menaces de sécurité potentielles.

Indicateurs

Score des contrôles des configurations PCI

Affiche le score des contrôles des configurations PCI de votre instance sous forme de pourcentage. Ce pourcentage représente le pourcentage de configurations de contrôle PCI de sécurité sur votre instance qui répondent aux normes de conformité. L'indicateur affiche également la date à laquelle le score de conformité a été calculé et une comparaison avec le score calculé précédent.

Visualisation des données

Titre	Type	Table source	Description
Contrôles des configurations PCI	 Graphique à barres empilées	Configurations de sécurité [isc_security_configurations]	Affiche les configurations de contrôle PCI conformes et non conformes dans les catégories élevée, moyenne et faible. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

Rechercher des définitions de sécurité incorrectes

Exécutez l'auditeur pour analyser votre instance et trouver des définitions de sécurité incorrectes. Elle fournit des résultats que vous pouvez corriger pour améliorer la posture de sécurité de votre instance.

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

L'auditeur effectue une évaluation « complète » de l'intégrité de votre instance qui analyse la configuration de votre système. Pour les analyses de sécurité, il compare votre configuration de sécurité actuelle aux définitions de bonnes pratiques et aux valeurs de conformité des propriétés de sécurité.

Du point de vue de la sécurité de l'instance, il fournit des informations et des recommandations sur ce que vous devez continuer à faire et sur les points que vous pouvez améliorer. Ces informations et recommandations vous aident à répondre aux questions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les propriétés appropriées liées à la sécurité sont-elles définies ?
- Le module d'extension de haute sécurité est-il activé ?
- Existe-t-il des règles de contrôle d'accès appropriées ?

Exécuter l'auditeur et analyser les résultats de l'analyse

1. Pour exécuter l'auditeur, cliquez sur **Audit** sur la page d'accueil du Centre de sécurité de l'instance.
2. Une fois l'analyse terminée, ouvrez les résultats de l'analyse pour examiner et analyser les résultats de sécurité.
3. Pour examiner les détails d'un résultat d'analyse spécifique, double-cliquez sur le numéro de résultat. Ces informations comprennent son état, le type d'analyse, la durée d'exécution et les messages d'erreur.
4. Chacune des conclusions de l'auditeur contient des détails sur la résolution et une URL vers le contenu du produit sur la manière de les traiter. Suivez les instructions documentées pour résoudre les problèmes dans chacune des conclusions.

Information associée

Paramètres de sécurisation renforcée

Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3]

Règles de la liste de contrôles d'accès

Surveiller les mesures d'instance

Surveillez les mesures d'utilisateur, d'exportation, d'authentification, d'e-mail et d'antivirus pour votre instance. Par exemple, vous pouvez surveiller la sécurité de vos e-mails en vérifiant les mesures de spam, d'e-mails externes et d'e-mails entrants provenant de domaines non approuvés et de confiance pour votre instance. Analysez ces mesures pour rechercher des comportements de sécurité anormaux liés aux activités qui ont lieu dans votre instance.

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

Mesures des utilisateurs

Analysez les mesures utilisateur pour rechercher des comportements anormaux liés à des types spécifiques d'activité utilisateur dans votre instance.

Non connecté le mois dernier / Six derniers mois / L'année dernière

Indique le nombre d'utilisateurs qui ne se sont pas connectés à l'instance au cours du dernier mois, des six derniers mois et de la dernière année civile. Pour afficher les détails de l'utilisateur pour une mesure spécifique :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur la mesure pour afficher une liste des utilisateurs qui ne se sont pas connectés à l'instance pendant la période indiquée.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet utilisateur.

Utilisateurs avec rôles de privilège élevé

Indique le nombre d'utilisateurs avec les types de rôles de privilège élevé suivants :

Rôle d'utilisateur	Description
administrateur	Rôle d'administrateur principal ayant accès à l'ensemble des données, fonctions et fonctionnalités système, quelles que soient les contraintes de sécurité.
ais_high_security_admin	Rôle à privilège élevé qui permet à un utilisateur d'accéder aux paramètres de haute sécurité pour Recherche IA. Pour en savoir plus, consultez Affecter des rôles à Recherche IA Administrateurs et utilisateurs .
password_reset_admin	Rôle d'administrateur qui permet à un utilisateur d'afficher l'état des activités de réinitialisation du mot de passe, d'identifier les menaces potentielles pour la sécurité et de surveiller la conformité avec les politiques de sécurité des mots de passe. Pour en savoir plus, consultez Réinitialisation du mot de passe et les rapports et journaux sur les changements de mot de passe .
script_include_admin	Rôle d'administrateur qui a également accès aux includes de script.
security_admin	Rôle à privilège élevé qui permet à un utilisateur de créer et de modifier des contrôles d'accès et des paramètres de sécurité élevée. Pour en savoir plus, reportez-vous à la rubrique Security_admin rôle.
user_admin	Rôle d'administrateur qui permet également de gérer les utilisateurs, les rôles, les groupes d'utilisateurs, les rôles et les affectations de département.

Remarque :
Pour en savoir plus sur ces types de rôles administratifs, consultez Rôles administratifs spéciaux .

Pour afficher les détails de l'utilisateur pour une mesure de rôle d'utilisateur spécifique :

- Cliquez sur la mesure du rôle du nombre d'utilisateurs pour afficher une liste des utilisateurs disposant de ce type de rôle de privilège élevé.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet utilisateur. Vous pouvez ensuite déterminer si ces rôles critiques pour la sécurité sont affectés au personnel approprié.

Tendance des utilisateurs

Affiche les informations de tendance du nombre sur une période pour les types d'utilisateurs suivants :

Type de nombre	Description
Utilisateurs actifs	Nombre d'utilisateurs marqués comme actifs dans l'instance.
Utilisateurs inactifs	Nombre d'utilisateurs marqués comme inactifs dans l'instance.
Verrouillé	Nombre d'utilisateurs bloqués hors de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher les détails d'un utilisateur pour un nombre d'utilisateurs spécifique (par exemple, Utilisateurs bloqués) :

- Cliquez sur la mesure **Utilisateurs bloqués** .
- Dans la page, cliquez sur Afficher les Centre d'analyse**enregistrements**.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet utilisateur. Vous pouvez alors déterminer s'il y a une raison pour laquelle cette personne est verrouillée et remédier à la situation.

Tendance des événements

Affiche les informations de tendance du nombre pour des types d'événements spécifiques, sur une période donnée :

Type d'événement	Description
Connexion de l'administrateur	Nombre d'utilisateurs avec des rôles d'utilisateur administrateur aux privilèges élevés qui se sont connectés un jour spécifique.
Connexion externe	Nombre d'utilisateurs avec un rôle de snc_external affecté qui se sont connectés à cette instance au cours de la journée calendaire. Ces connexions ont généralement lieu à des fins de maintenance, de support, de conseil ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et non des problèmes de sécurité potentiels.
Échec de la connexion	Nombre d'échecs de tentatives de connexion un jour spécifique.
Emprunt d'identité	Nombre d'utilisateurs connectés un jour spécifique qui empruntent l'identité d'autres utilisateurs.
Élévation de sécurité	Nombre de fois qu'un administrateur de sécurité a élevé la sécurité pour les utilisateurs standard en changeant le rôle d'utilisateur qui leur est affecté en un rôle de sécurité avec privilège élevé au cours de la journée calendaire. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, administrateur, security_admin et emprunteur d'identité.
Connexion SNC	Nombre de personnes qui se sont connectées à cette instance à l'aide de la technique hi-hopping Service client et assistance au cours d'un jour spécifique.

Pour afficher les détails de l'utilisateur pour un nombre d'événements spécifique (par exemple, Emprunt d'identité) :

- Cliquez sur la mesure du nombre d'utilisateurs. La page Journaux des événements du tableau de bord de sécurité répertorie les journaux des événements pour ce type d'événement.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet événement.

Information associée

Centre d'analyse

Mesures d'exportation

Analysez les mesures d'exportation pour voir quelles données sont les plus couramment exportées et quels utilisateurs exportent le plus de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. **Exporter le graphique**

   Chaque rapport affiche le nombre d'événements d'exportation par date, à l'aide d'un code couleur pour indiquer quels utilisateurs ont effectué l'exportation. Cliquez sur une section colorée d'une colonne pour afficher la liste des enregistrements **d'événements d'exportation** [isc_export_event] correspondant à cette entrée.

2. **Signaler la clé**

   La clé en bas du rapport indique quelles couleurs identifient quels utilisateurs ou tables.

3. **Prévisualiser la fenêtre contextuelle**

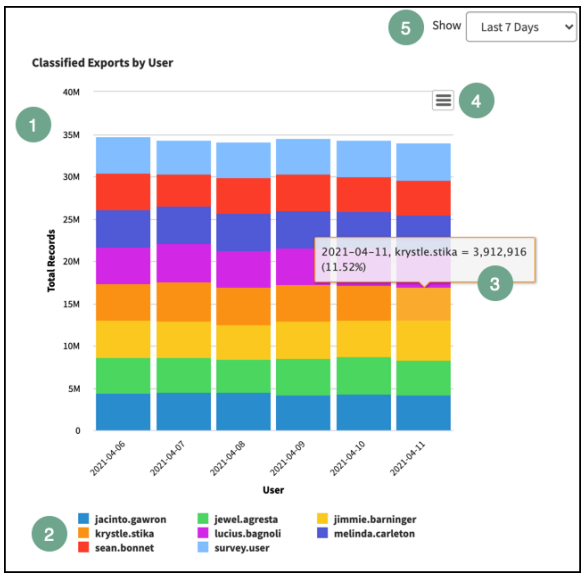
   Pointez sur une entrée dans le graphique pour afficher un aperçu contextuel. Cet aperçu affiche le nom de l'utilisateur ou de la table, ainsi qu'un nombre d'exportations et un pourcentage du total dans cette colonne.

4. **Exportation d'images**

   Cliquez sur l'icône pour enregistrer le rapport en tant qu'image. Vous pouvez enregistrer le rapport au format PNG ou JPEG.

5. **Plage de dates du rapport**

   Utilisez **Afficher la** liste pour afficher les exportations des dernières 24 heures ou des 7 derniers jours.



Exporter des rapports de mesures

La page Mesures d'exportation affiche quatre rapports.

Exportations par utilisateur

Utilisez le rapport **Exportations par utilisateur** pour voir lequel de vos utilisateurs exporte le plus de données.

Exportations classées par utilisateur

Utilisez le rapport **Exportations classées par utilisateur** pour voir lequel de vos utilisateurs exporte le plus de classifications de correspondance de données comme les informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées dans ce rapport dans l'onglet **Paramètres** .

Exportations par table

Utilisez le rapport **Exportations par table** pour voir à partir des tables les plus fréquemment exportées.

Exportations classées par table

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le rapport **Exportations classées par table** pour identifier les tables à partir desquelles vous exportez le plus souvent et qui correspondent à des classifications telles que les informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées dans ce rapport dans l'onglet **Paramètres** .

Remarque :
Les rapports de mesures d'exportation suivent uniquement les événements d'exportation. Les exportations à partir d'autres sources, telles que les API REST ou les workflows, ne sont pas suivies dans le cadre de cette fonctionnalité.

Exporter les paramètres des mesures

Utilisez les options de configuration de l'onglet Paramètres pour affiner les résultats du reporting.

Accédez aux paramètres de vos mesures d'exportation en cliquant sur l'onglet **Paramètres** .

Champs de configuration des paramètres

Exporter les configurations des mesures

Configuration	Description
Classifications des mesures	Ajoutez ou supprimez des classifications à ce champ pour déterminer quelles exportations sont incluses dans les rapports **Exportations classées par utilisateur** et **Exportations classées par table** . Ces rapports prennent en charge les classifications suivantes : • Informations personnellement identifiables • Confidentiel • Restreint • Interne • Public Pour plus de détails sur les classifications des données, voir Classifications des données
Classifications des alertes	Ajoutez ou supprimez des classifications à ce champ pour déterminer quelles exportations déclenchent des notifications de sécurité d'instance. Les classifications prises en charge dans le champ **Classifications des mesures** sont prises en charge ici. Pour en savoir plus sur ces alertes, reportez-vous à la section Notifications de sécurité de la Centre de sécurité de l'instance page. Le champ **Seuil d'enregistrement** définit le nombre d'enregistrements exportés avant que votre instance ne se déclenche et ne déclenche une alerte.
Seuil d'enregistrement	Nombre d'enregistrements qu'un utilisateur doit exporter pour déclencher une alerte. Pour déclencher une alerte, ces enregistrements doivent également correspondre aux classifications répertoriées dans le champ **Classifications des alertes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le bouton **Enregistrer** (⌘ **+ s)** pour enregistrer vos paramètres.

Mesures d'authentification

Analysez les mesures d’authentification pour afficher des informations relatives à l’authentification, telles que les adresses IP rarement utilisées, les échecs de connexion et les types de schémas d’authentification utilisés par vos utilisateurs.

Utilisez la page **Mesures d’authentification** pour afficher les rapports relatifs à votre configuration d’authentification. Les rapports suivants s’affichent dans cet onglet.

Remarque :
La page des mesures d’authentification nécessite le **module d’extension Politique d’accès de l’API REST** (com.glide.rest.policy). Pour plus d’informations sur cette fonctionnalité, consultez Politiques d’accès de l’API REST.

API sans politiques d’authentification

Affiche un nombre en temps réel de toutes les API sans politique d’accès

Sécurisation renforcée : flux de récupération du compte

Sécurisation renforcée : paramètre lié à la fonctionnalité MFA basée sur les rôles

Comptes d’accès au service Web uniquement

Affiche le nombre de tous les enregistrements utilisateur avec l’option d’accès au service Web activée dans `User` la table [sys_user].

Certificats X509 arrivant à expiration dans 30 jours

Affiche le nombre de tous les certificats X.509 de `X.509 Certificates` la table [sys_certificate] qui doivent expirer dans 30 jours.

Mesures d'authentification adaptative

Analysez les mesures d’authentification adaptative pour surveiller et ajouter des informations sur la façon dont l’authentification adaptative est utilisée sur votre instance.

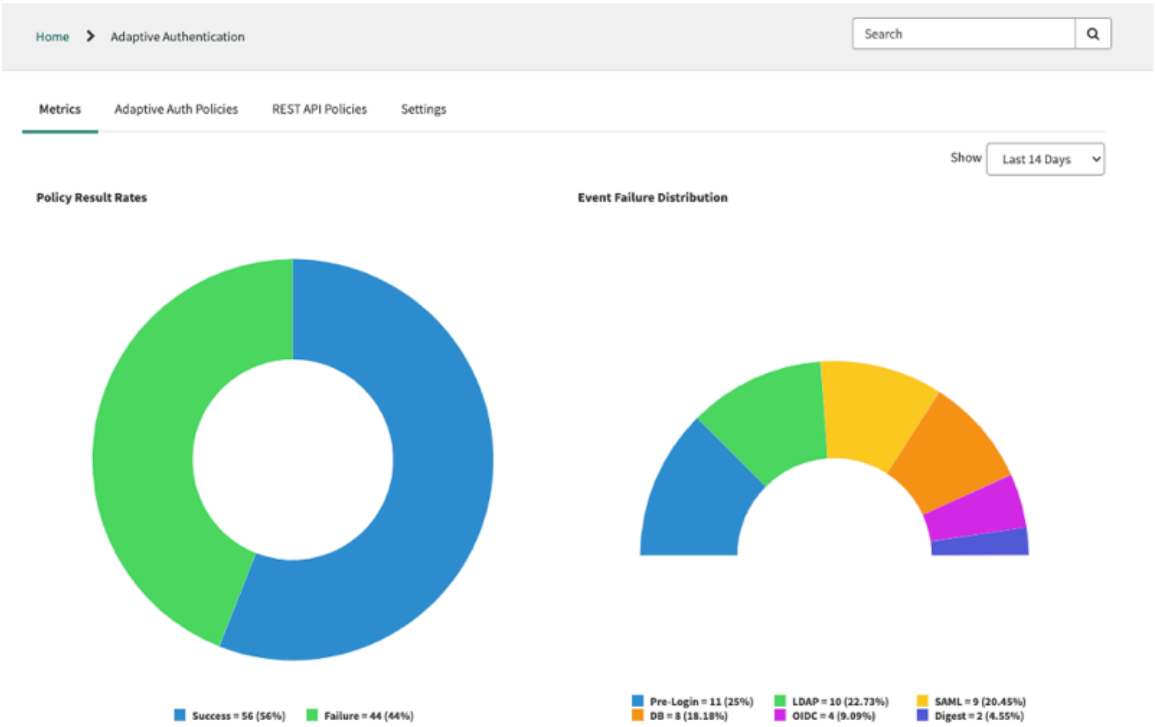
Affichez les rapports, les paramètres et les politiques associés à l’authentification adaptative en place à l’aide de la page Mesures d’authentification adaptative. Les administrateurs de sécurité peuvent utiliser des rapports pour surveiller les résultats de leurs politiques d’authentification adaptative. Utilisez ces données pour obtenir des informations et adapter vos politiques afin d’améliorer leurs performances.

Remarque :
La page des mesures d’authentification adaptative nécessite le module d’extension **Authentification adaptative** (com.snc.adaptive_authentication). Pour en savoir plus sur cette fonctionnalité, reportez-vous à la rubrique Authentification adaptative.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures



Utilisez l'onglet **Mesures** pour afficher les rapports relatifs à votre configuration d'authentification adaptative. Les rapports suivants s'affichent dans cet onglet.

- Taux de résultats de la politique
- Distribution d'échecs d'événements
- Distribution de la réussite d'événement
- Adresses IP refusées
- Connexions des utilisateurs authentifiés
- Connexions des utilisateurs de l'API
- Tendance en matière d'authentification

Utilisez Afficher la liste pour sélectionner une période pour les rapports affichés

Politiques d'authentification adaptative

Utilisez l'onglet **Politiques d'authentification adaptatives** pour afficher les politiques d'authentification adaptative et les contextes de politique sur votre instance. Cliquez sur une entrée de ces listes pour afficher l'enregistrement associé. Pour en savoir plus sur ces enregistrements, consultez Authentification adaptative

Paramètres

Utilisez l'onglet Paramètres pour afficher et configurer les propriétés système de l'authentification adaptative. Pour plus d'informations sur ces propriétés, voir Configurer les propriétés d'authentification adaptative

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures d'e-mail

Analysez vos mesures d'e-mail pour rechercher des comportements anormaux liés aux e-mails entrants dans votre instance. Par exemple, si les mesures indiquent un pic d'e-mails de spam provenant de domaines spécifiques, vous pouvez définir des actions entrantes qui empêchent leur livraison à l'instance.

Pour chaque mesure d'e-mail, un nombre s'affiche pour chaque type d'e-mail remis ou envoyé à l'instance au cours de la journée calendaire.

Préférence de notification	Description
E-mail entrant externe	Nombre d'e-mails entrants pour le jour du calendrier qui ont été remis à l'instance à partir de domaines de messagerie externes. **Remarque :** Les domaines d'e-mail externes sont les domaines qui ne sont pas répertoriés dans la propriété système, car cette propriété suit uniquement vos domaines d'e-mail `security.list.internal.domains` internes. Pour en savoir plus sur cette propriété, consultez Propriétés système disponibles .
Courrier indésirable	Nombre d'e-mails entrants pour le jour du calendrier qui ont été remis à l'instance et marqués comme courrier indésirable. Un nombre qui ne correspond pas aux tendances historiques peut indiquer que des tentatives sont faites pour compromettre la sécurité de votre instance.
E-mail entrant approuvé	Nombre d'e-mails entrants vers l'instance pour le jour du calendrier en provenance de domaines d'e-mail désignés comme approuvés.
E-mail entrant non approuvé	Nombre d'e-mails entrants à l'instance pour le jour civil en provenance de domaines d'e-mail désignés comme non approuvés. Vous pouvez désigner des domaines de messagerie non approuvés ou de confiance dans le formulaire Domaine non approuvé et approuvé afin de pouvoir suivre les e-mails entrants qui sont envoyés à partir de ces derniers. Pour savoir comment désigner des domaines de messagerie non approuvés ou de confiance, reportez-vous à la section Désigner des domaines d'e-mail comme n'étant pas de confiance ou n'étant pas de confiance.

Après avoir cliqué sur une mesure d'e-mail, vous pouvez en savoir plus sur les problèmes de sécurité de messagerie possibles dans votre instance en cliquant sur l'un des onglets suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commande	Description
Graphique	Nombres d’e-mails entrants et tendances du nombre dans le temps pour le type d’e-mail sélectionné (courrier indésirable, externe entrant, non approuvé ou approuvé).
Enregistrements	Enregistrements d’e-mails individuels qui compromettent le nombre quotidien pour le type d’e-mail sélectionné.
Plus d'informations	Informations supplémentaires pour le type d’e-mail sélectionné.

Remarque :
Les mesures d’e-mail s’appliquent uniquement aux e-mails entrants que vous envoyez à l’instance. Les mesures ne s’appliquent pas au trafic normal traité via les serveurs de messagerie de votre entreprise. Pour en savoir plus sur la définition des actions entrantes et leur impact sur le traitement de vos e-mails entrants, consultez Actions sur e-mail entrant .

Désigner des domaines d’e-mail comme n’étant pas de confiance ou n’étant pas de confiance

Désignez des domaines d’e-mail spécifiques comme non approuvés ou de confiance afin que vous puissiez surveiller les mesures des e-mails entrants provenant de ces sources dans votre instance.

Avant de commencer
Rôle requis : security_dashboard_user ou admin

Pourquoi et quand exécuter cette tâche
Lorsque des domaines non approuvés ou de confiance envoient des e-mails à votre instance, leur nombre quotidien apparaît dans les mesures **E-mail entrant non approuvé** ou **E-mail entrant de confiance** sur la page E-mail. Vous pouvez ensuite suivre l’activité des e-mails de ces domaines et utiliser les journaux d’e-mails pour afficher des e-mails entrants spécifiques. Vous pouvez également spécifier un utilisateur, généralement un gestionnaire ou un analyste de sécurité, pour vous informer chaque fois qu’une activité se produit à partir du domaine non approuvé ou approuvé.

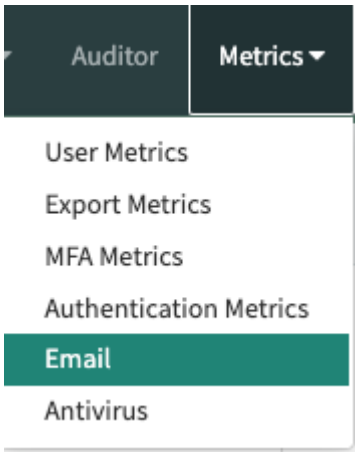
Remarque :
La désignation d’un domaine de messagerie comme non approuvé n’est utilisée qu’à des fins de suivi de sécurité. Les administrateurs peuvent également configurer un filtre d’adresse système pour ignorer les e-mails provenant de domaines non approuvés. Pour en savoir plus sur le filtrage des e-mails pour bloquer leur remise, consultez Filtres d’adresse du système .

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Sur la page d’accueil du Centre de sécurité de l’instance, sélectionnez **E-mail** dans le menu **Mesures** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



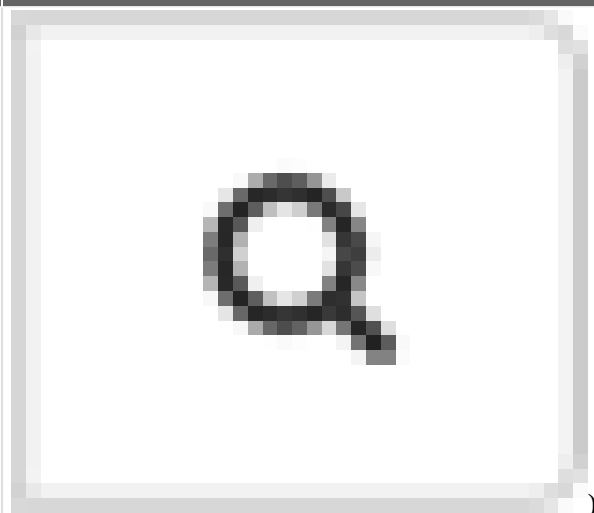
3. Sur la page E-mail, dans la section Domaines non approuvés et approuvés, cliquez sur **Nouveau**.
4. Remplissez les champs du formulaire.

Formulaire de domaine non approuvé et approuvé

Champ	Description
Domaine	Nom du domaine de messagerie que vous désignez comme n'étant pas de confiance ou non approuvé. Par exemple, saisissez servicenow.com pour désigner ServiceNow des employés qui peuvent envoyer des e-mails de confiance à l'instance.
Catégorie	Catégorie qui indique si le domaine de messagerie n'est pas approuvé ou approuvé : **Non approuvé** Indique que le domaine de messagerie n'est pas de confiance. Vous l'utilisez pour identifier les domaines qui envoient des messages suspects ou les e-mails qui constituent une menace de sécurité potentielle pour l'instance. **Approuvé** Indique que le domaine de messagerie est de confiance. Vous l'utilisez pour identifier des domaines lorsque vos mesures indiquent que les e-mails entrants en provenance de celui-ci ne présentent aucune menace pour la sécurité. La désignation du domaine comme étant de confiance vous permet de suivre l'activité des e-mails entrants au fil du temps.
Actifs	Cochez la case pour activer ou désactiver le statut non approuvé ou approuvé pour le domaine de messagerie spécifié.
Notify	Nom de l'utilisateur à notifier par e-mail lorsqu'une activité se produit dans le domaine non approuvé ou approuvé. Cliquez sur l'icône de recherche Spotlight (

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	) pour rechercher le nom de l’utilisateur. Laissez le champ **Notification** vide si vous ne souhaitez pas que des notifications soient envoyées.

5. Sélectionnez **Enregistrer**.

Résultats

Les informations sur les domaines d’e-mail non approuvés ou approuvés sont également ajoutées à la liste **des domaines non approuvés et approuvés** sur la page E-mail.

Information associée

Centre de sécurité de l'instance

Mesures d’e-mail

Mesures antivirus

Si le module d’extension est activé, Analyse antivirus il s’exécute Analyse antivirus dans votre instance pour la protéger contre les infections virales provenant des pièces jointes.

Les mesures suivantes s’affichent pour les 60 derniers jours d’activité et vous permettent d’évaluer l’efficacité des Analyse antivirus fonctions.

Événements antivirus

Les événements antivirus indiquent le nombre d’événements antivirus dans votre instance, par date. Pour accéder aux événements antivirus, accédez à **Sécurité de système** > **Centre de sécurité de l'instance** et sélectionnez l’onglet Mesures. Les lignes de graphique à code couleur représentent les types d’événements antivirus suivants :

Couleur	Description
Bleu	Nombre de fichiers mis en quarantaine par Analyse antivirus dans cette instance pour la date indiquée.
Vert	Nombre de fichiers infectés téléchargés sur l’instance, puis mis en quarantaine pour la date indiquée. Ces fichiers sont principalement des pièces jointes d’e-mail qui contiennent un virus ou un code rouge.
Jaune	Nombre de fichiers mis en quarantaine dans l’instance qui ont été supprimés pour la date indiquée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Couleur	Description
Orange	Nombre de fichiers mis en quarantaine dans l'instance qui ont été restaurés pour la date indiquée. **Remarque :** Après l'exécution Analyse antivirus et la détection de faux positifs, vous pouvez restaurer un fichier en quarantaine et le rendre accessible dans l'instance.

- Pour accéder à la Centre d'analyse page et afficher la carte de score détaillée et les informations d'analyse pour une date spécifique, cliquez sur une ligne colorée dans le graphique Événements antivirus. Par exemple, cliquez sur la ligne graphique bleue pour afficher les informations d'analyse des fichiers mis en quarantaine pour une date spécifique.
- Pour afficher les répartitions suivantes dans la page, cliquez sur Centre d'analyse Répartition , puis sur :

Répartition	Description
AppSec : source de l'événement antivirus	Source de l'événement antivirus. ○ **Au chargement :** S'est produit en raison du chargement d'un fichier infecté, généralement une pièce jointe. ○ **À partir de la quarantaine :** S'est produit en raison de la mise en quarantaine d'un fichier infecté, généralement une pièce jointe. ○ **Au téléchargement :** S'est produit en raison du téléchargement d'un fichier infecté, généralement une pièce jointe. ○ **À partir de l'enregistrement :** S'est produit en raison d'un enregistrement infecté dans une table.
AppSec : type d'événement antivirus	Type d'événement antivirus. ○ **Quarantaine:** S'est produit en raison de la mise en quarantaine d'un fichier, généralement une pièce jointe. ○ **Téléchargé:** S'est produit en raison du téléchargement d'un fichier, généralement une pièce jointe. ○ **Restauré:** S'est produit en raison de la restauration d'un fichier mis en quarantaine. ○ **Supprimé:** S'est produit en raison de la suppression d'un fichier en quarantaine.
AppSec : outil de téléchargement d'antivirus	Nom de l'utilisateur connecté qui a téléchargé les fichiers qui sont à l'origine des infections virales détectées par l'application Analyse antivirus .

Fichiers en quarantaine

Répertorie les fichiers infectés dans l'instance mise en quarantaine par Analyse antivirus:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom de fichier	Nom du fichier infecté.
Type de contenu	Type de contenu infecté dans le fichier. Par exemple, **application/x-dosexec** est une application infectée ou un fichier exécutable DOS, tandis que **text/plain** est un fichier .txt infecté.
Table	Nom de la table qui contient le fichier infecté. Par exemple, **incident** s'affiche pour un enregistrement de fichier d'incident.
Virus	Nom du fichier mis en quarantaine par Analyse antivirus.
Détectée	Date et heure auxquelles le fichier infecté a été détecté.
Créés par	Nom de l'utilisateur qui a mis en quarantaine le fichier infecté.
Créées	Date et heure de création de l'enregistrement de fichier de quarantaine.
ID système de table	Identificateur de système de table affecté à l'enregistrement de fichier de quarantaine.

Remarque :
Vous pouvez également ajouter des tuiles **Fichiers en quarantaine** et **Types de virus** au ruban Événement. Pour en savoir plus, reportez-vous aux sections Surveiller les événements de sécurité et Configurer le ruban d'événement de sécurité.

Information associée

- Analyse antivirus
- Configurer Analyse antivirus
- Examen des fichiers en quarantaine
- Examiner l'activité antivirus
- Centre d'analyse
- Répartitions d'Analyse des performances
- Analytics, Intelligence and Reporting

Tableau de bord des mesures MFA

Le tableau de bord des mesures MFA affiche des informations sur la configuration de l'authentification multifacteur de vos instances. Utilisez le tableau de bord pour vous assurer que votre configuration MFA répond à vos normes de sécurité.

Rôles ServiceNow AI Platform requis

security_dashboard_user ou administrateur nécessaire pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des mesures MFA

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l'instance, cliquez sur **Mesures** dans l'en-tête, puis sélectionnez **Mesures MFA**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité de la sécurité des instances.
Admin (admin)	Surveillez en permanence la conformité de la sécurité de l'instance pour détecter les menaces de sécurité et y répondre.

Indicateurs

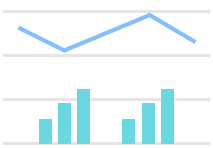
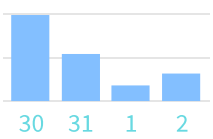
Utilisateurs inscrits pour MFA

Affiche le nombre total d'utilisateurs sur l'instance inscrits à la MFA . Cliquez pour ouvrir le centre d'analyse pour plus d'informations.

Utilisateurs utilisant le contournement de la MFA

Affiche le nombre total d'utilisateurs utilisant le contournement de la MFA. Cliquez pour ouvrir le centre d'analyse pour plus d'informations.

Visualisations des données

Titre	Type	Table source	Description
Utilisateurs MFA aux privilèges élevés			
Tendance des utilisateurs de MFA	 Graphique de tendance		

Activer l'interface ISC Agent virtuel

Si vous disposez du rôle administrateur, vous pouvez activer le module d'extension ISC Agent virtuel Conversations (com.glide.isc_virtualagent). L'activation de ce module d'extension installe les packs de Agent virtuel contenu and Compréhension du langage naturel (NLU , fournissant un Agent virtuel accès à partir du Centre de sécurité de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Important :

Le centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers la ServiceNow Centre de sécurité migration.

L'interface Agent virtuel dans Centre de sécurité de l'instance n'est disponible que pour les utilisateurs avec des abonnements payants Agent virtuel et qui ont activé le module d'extension Agent virtuel Glide (com.glide.cs.chatbot). Pour en savoir plus, consultez Activer l'Agent virtuel .

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

L'interface ISC Agent virtuel vous permet d'effectuer les tâches suivantes :

- Posez des questions liées à la sécurité, puis obtenez des réponses récapitulatives rapides et des liens de référence pour en savoir plus.
- Obtenez des réponses relatives au Centre de sécurité de l'instance, à la sécurité de la plateforme, aux politiques de sécurité ServiceNow, à la confiance, à la gouvernance, au risque et à d'autres processus.
- Recherchez des ressources liées à la sécurité, telles que des rubriques de la base de connaissances dans le portail de sécurité Now Support.

Modules d'extension pour ISC Agent virtuel

Module d'extension	Description
ISC Agent virtuel Conversations [com.glide.isc_virtualagent]	Active le pack de contenu Conversations ISC Agent virtuel pour Centre de sécurité de l'instance.
Modèle ISC NLU pour Agent virtuel les conversations [com.glide.isc_nlu]	Active le pack de Compréhension du langage naturel contenu (NLU) pour le Centre de sécurité de l'instance.

Remarque :

L'activation du module d'extension com.glide.isc_virtualagent active automatiquement com.glide.isc_nlu. Toutefois, si vous activez d'abord le module d'extension com.glide.isc_nlu, vous devez également com.glide.isc_virtualagent activer manuellement.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Paramètres de sécurisation renforcée

Le contenu des ServiceNow paramètres de sécurisation renforcée du Centre de sécurité (SSC) contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le ServiceNow AI Platform. Vous pouvez définir ces propriétés à l'aide de l'application Paramètres de sécurisation renforcée du Centre de sécurité.

Vue d'ensemble et objectif

Le Centre de sécurité calcule un score de conformité quotidien, exprimé en pourcentage, qui est basé sur le degré de conformité des paramètres de sécurité de votre instance actuelle avec les valeurs de conformité des paramètres de sécurisation renforcée du Centre de sécurité.

Vous pouvez gérer les paramètres de configuration de sécurité spécifiques susceptibles d'affecter le score de votre instance directement à partir du Centre de sécurité.

Les configurations des paramètres de sécurisation renforcée sont expliquées à l'aide de plusieurs attributs décrits dans le tableau.

Détails de la configuration des paramètres de sécurisation renforcée

Attribut de configuration	Description
Vue d'ensemble	Fournit une vue d'ensemble de haut niveau de la recommandation.
Nom de la configuration	Le nom de la propriété ou du module d'extension.
Type de configuration	Décrit où la propriété peut être configurée en dehors du centre de sécurité, par exemple dans les propriétés système (*sys_properties_list.do*).
Type de données	Décrit le type de valeur requis pour la configuration. Les exemples sont vrai/faux booléen, installation, module d'extension, chaîne, et autres.
Valeur recommandée	Valeur recommandée par le Centre de sécurité pour améliorer la conformité de la sécurité dans votre instance.
Valeur par défaut	La valeur sur laquelle la configuration est définie dans le système de base.
Catégorie	Nom et lien vers la catégorie du paramètre de sécurisation renforcée.
Risque de sécurité	**Score de gravité** : le score indique le risque de sécurité potentiel pour votre instance en fonction de la probabilité d'exploitation de la vulnérabilité. La vulnérabilité de sécurité est examinée et notée individuellement à l'aide du score CVSS (Common Vulnerability

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de la configuration des paramètres de sécurisation renforcée (suite)

Attribut de configuration	Description
	Scoring System) sur une échelle allant de **0,0** à **10,0**. Consultez https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator pour plus d'informations.
	Évaluation de gravité par score CVSS : • Critique : 9,0 à 10,0 • Élevé : 7,0 à 8,9 • Moyen : 4,0 à 6,9 • Faible : 0,01-3,9 • Aucun : 0,0
	Détails du risque de sécurité : décrit l'importance de la configuration des paramètres et le risque de ne pas utiliser la configuration recommandée.
Dépendances et prérequis	Paramètres ou configurations connexes requis avant ou en conjonction avec la configuration de sécurisation renforcée.
Impact fonctionnel	Impact de ce paramètre de sécurisation renforcée sur le fonctionnement de votre instance.
Références	Liens vers la documentation de configuration ou d'autres informations utiles.

Remarque :
Certaines configurations ne peuvent être complétées que par Service client et assistance et seront indiquées comme telles.

Pour en savoir plus sur la façon de garantir que vos instances répondent aux exigences de sécurisation renforcée, reportez-vous à la section Sécurisation renforcée de la sécurité.

Autres ressources

Pour la référence utilisateur, la ServiceNow AI Platform conserve des informations détaillées sur les options de configuration dans la documentation du produit. Les liens trouvés dans Sécuriser votre instance vous permettent d'accéder à la plupart du contenu de la sécurité. Consultez également les rubriques suivantes :

- Propriétés système disponibles
- Propriétés des paramètres de sécurité généraux
- Paramètres de sécurité élevée

Paramètres de sécurisation renforcée Versions de base de référence

Découvrez comment les versions de base de référence pour les paramètres de sécurisation renforcée s'alignent sur les versions de famille et de stockage.

Centre de sécurité Fonctionne en ingérant un sous-ensemble de propriétés système à partir d'une instance et en affichant ses détails de configuration, ainsi que l'impact sur la sécurité de la non-conformité au sein de l'application. La base de référence sert de point de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

référence pour les propriétés système ingérées avec chaque version de l'application Centre de sécurité.

Vue d'ensemble de la base de référence des paramètres de sécurisation renforcée

Version du centre de sécurité	Version de base de référence des paramètres de sécurisation renforcée	Familles prises en charge	Date de mise en production du magasin	Installé par défaut avec
SSC v1.1	Base de référence v1.0	Utah, Vancouver	mai 2023	Famille de Vancouver
SSC v1.2	Base de référence v1.0	Utah, Vancouver	août 2023	Stocker uniquement
SSC v1.3	Base de référence v2.0	Vancouver, Washington DC	nov. 2023	Famille Washington
SSC v1.5	Base de référence v4.0	Washington DC, Xanadu	mai 2024	Xanadu
SSC v1.6	Base de référence v4.0	Washington DC, Xanadu	Août 2024	Stocker uniquement
SSC v 2.0	Base de référence v5.0	Xanadu, Yokohama	Novembre 2024	Yokohama

Nouveaux paramètres de sécurisation renforcée

Les nouveaux paramètres de sécurisation renforcée sont répartis par version de base.

Nouveaux paramètres de sécurisation renforcée pour la base de référence 7.0

De nouveaux paramètres de sécurisation renforcée ont été publiés avec la version de base de référence 7.0 du Centre de sécurité.

- Activer les vérifications de privilège entre périmètres sur le formulaire du portail de services [Nouveautés dans Security Center 7.0]
- Valider les ACL de requête sur les fonctions de base de données Glide [nouveau dans Security Center 7.0]
- Utiliser la classification de documents pour limiter les documents accessibles au public [nouveau dans Security Center 7.0]
- Restreindre l'accès en écriture aux champs système pour les utilisateurs administrateurs [nouveau dans Security Center 7.0]
- Exiger l'approbation pour les changements d'appartenances aux groupes Office 365 basés sur des agents [Nouveau dans Security Center 7.0]
- Exclure les tables et champs sensibles de la génération de données [nouveau dans Security Center 7.0]
- Appliquer les rôles de lecture pour la recherche de variables de catalogue [Nouveautés de Security Center 7.0]
- Appliquer un choix de chaîne de requête valide [Nouveau dans Security Center 7.0]
- Fonctionnalité de liaison restreinte en cas d'autorisation du titulaire [nouveau dans le centre de sécurité 7.0]
- Désactiver les informations d'identification du mot de passe du propriétaire de ressource (ROPC) dans les attributions de jetons OAuth 2 [Nouveau dans Security Center 7.0]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Renforcer l’approbation de certificat [Mis à jour dans Centre de sécurité 1.3, supprimé dans la version 2.0, ajouté dans la version 7.0]
- Empêcher l’utilisation des clés 3DES [nouveau dans Security Center 7.0]
- Autorisez les liens HTML vers des domaines de confiance dans les champs de description du module de l’espace de travail Impact [nouveau dans Security Center 7.0]
- Garantir que la recherche contextuelle ne contient pas de redirection non validée [nouveau dans Security Center 7.0]
- Nettoyer le HTML dans les champs de description du module de l’espace de travail Impact [Nouveau dans Security Center 7.0]

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 6.0

De nouveaux paramètres de sécurisation renforcée ont été publiés avec la version de base de référence 6.0 du Centre de sécurité.

- Appliquer des ACL spécifiques à l’application uniquement pour les données d’application
- Désactiver l’utilisation de l’interface utilisateur JQuery héritée
- Afficher des recommandations pour les pages d’interface utilisateur à risque élevé
- Appliquer les exigences actuelles de conformité à la politique de mot de passe lors de la connexion
- Empêcher les utilisateurs d’accepter l’avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]
- Définir la longueur minimale du mot de passe [Mis à jour dans Centre de sécurité 2.2]
- Limiter la durée de la session pour les sessions d’assurance élevée
- Désactiver les versions TLS déconseillées
- Désactiver la connexion locale pour les utilisateurs avec l’authentification unique (SSO) activée
- Réduire les contournements autorisés pour la configuration multifacteur
- Empêcher l’emprunt d’identité de l’utilisateur d’afficher les données de l’application
- Empêcher la journalisation des requêtes HTTP détaillées
- Activer l’état du relais dans les demandes SAML pour prévenir les attaques par relecture
- Minimiser les tentatives de connexion échouées pour les sessions d’assurance élevée
- Appliquer des politiques d’authentification continue aux sessions mobiles
- Désactiver l’utilisation de l’algorithme de chiffrement TripleDES/3DES

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 5.0

De nouveaux paramètres de sécurisation renforcée ont été publiés avec la version de base de référence 5.0 du Centre de sécurité.

- Appliquer l’ACL sur les données des événements de cycle de vie RH [nouveau dans Security Center 2.0]
- Nettoyer tous les champs HTML traduits [nouveau dans Security Center 2.0]
- Configurer la liste d’autorisation de widgets du portail de services [Nouveau dans le centre de sécurité 2.0]
- Appliquer l’ACL sur les données HR Core [nouveau dans Security Center 2.0]
- Appliquer l’ACL sur les données de l’Agent virtuel RH [nouveau dans Security Center 2.0]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurer la liste d'autorisation de la table des widgets du portail de services [nouveau dans Security Center 2.0]
- Appliquer le champ d'application de sécurité pour les informations d'application de service [nouveau dans Security Center 2.0]
- Empêcher la création d'ACL vide [nouveau dans le centre de sécurité 2.0]
- Empêcher l'accès non authentifié au client Web incorporé de l'agent virtuel
- Définir le nettoyage automatique des jetons pour les informations d'identification de jeton [nouveau dans Security Center 2.0]
- Restreindre le développement d'application global par rôle [nouveau dans Security Center 2.0]
- Activer les ACL pour une requête codée dans le widget de liste simple [nouveau dans Centre de sécurité 2.0]
- Invalider la session après l'expiration du jeton OAuth [nouveau dans Security Center 2.0]
- Définir les types MIME enfant autorisés [nouveau dans Centre de sécurité 2.0]
- Restreindre l'emprunt d'identité à l'administrateur [nouveau dans Security Center 2.0]

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 4.0

De nouveaux paramètres de sécurisation renforcée ont été publiés avec la version de base de référence 4.0 du Centre de sécurité.

- Examiner les conditions de contrôle d'accès au rôle explicite superflu [Supprimé dans Centre de sécurité 1.5]
- Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]
- Restreindre l'accès en lecture au contexte de flux [nouveau dans Security Center 1.5]
- Limiter l'intervalle de jeton d'actualisation mobile d'accès à la session basée sur une politique [Nouveau dans Security Center 1.5]
- Activer l'accès à la session basé sur des politiques pour mobile [Nouveau dans Security Center 1.5]
- Empêcher les utilisateurs inactifs de se connecter [nouveau dans le centre de sécurité 1.5]
- Configurer les rôles administrateur du groupe d'affectation de gestion des événements [nouveau dans Security Center 1.5]
- Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]
- Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 2.0

De nouveaux paramètres de sécurisation renforcée ont été publiés avec la version de base de référence 2.0 du Centre de sécurité.

- Assurez-vous que les ACL de table d'archivage sont vérifiées [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]
- Appliquer les restrictions du périmètre de l'application [nouveau dans Security Center 1.3 et supprimé dans la version 1.5]
- Activer le gestionnaire de sécurité Java renforcé [nouveau dans le centre de sécurité 1.3]
- Vérifier la révocation du certificat [nouveau dans Security Center 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Exiger l’effacement du presse-papiers lors de l’affichage l’application mobile en arrière-plan [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Activer le module d’extension Tables protégées [nouveau dans le centre de sécurité 1.3]
- Appliquer le privilège d’élévation stricte [nouveau dans Security Center 1.3]
- Limiter la durée de vie de la session active des intégrations [nouveau dans Security Center 1.3]
- Invalider de manière proactive les sessions inactives [nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]
- Activer le journal d’audit MID [nouveau dans Security Center 1.3 et mis à jour dans 1.5]
- Utilisation de l’opération multiple d’insertion sécurisée dans l’API de jeu d’importation [nouveau dans Security Center 1.3]
- Appliquer la vérification OCSP en cas d’erreur réseau [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]
- Appliquer des règles de sécurité au partage de tableaux de bord [nouveau dans Security Center 1.3]
- Restreindre les paramètres OAuth au corps POST [nouveau dans Security Center 1.3]
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction pour les points de terminaison GraphQL [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Désactiver le comportement hérité de clôture du champ d’application GlideRecord [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]
- Appliquer l’utilisation d’alias d’informations d’identification [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]
- Instanciateurs de connexions JMS requis [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Consigner les événements d’audit de session [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Exiger un accès en écriture pour accéder à la page Ajouter un élément du catalogue de services [Nouveau dans Security Center 1.3]
- Définir les rôles d’exception de délai d’expiration de session active [nouveau dans Security Center 1.3]
- Authentification basée sur certificat non mise en application [Nouveau dans Security Center 1.3]
- Appliquer l’accès ACL inclus dans le champ d’application pour les playbooks de demande d’informations [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Masquer les commentaires des utilisateurs sur les articles [nouveau dans Security Center 1.3]
- S’assurer que la création/la suppression des tableaux de bord nécessite une vérification d’accès [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]
- Appliquer les exigences relatives au chiffrement de l’appareil et au code d’accès [nouveau dans Security Center 1.3]
- Valider le type MIME de fichier dans AttachmentCreator SOAP Web Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Vérifier la révocation du certificat [nouveau dans Security Center 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifier l’emprunt d’identité dans l’évaluation ACL de l’application RH [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Exiger un captcha pour l’expérience de visite d’un invité dans l’application Service clientèle [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Exiger l’authentification sur le processeur HTTP de Gestion des événements [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]
- Limiter la durée de vie de la session active de l’invité [nouveau dans Security Center 1.3]
- Interdire le clonage cible [Nouveau dans Security Center 1.3]
- Définir une politique de sécurité de contenu sûre pour les fichiers SVG [Nouveau dans Security Center 1.3]
- Durée de validation du jeton anti-CSRF [Nouveau dans Security Center 1.3]
- Restreindre l’accès aux bases de connaissances [nouveau dans Security Center 1.3]
- Appliquer la sécurité du champ d’application pour les services digitaux du secteur public [nouveau dans Security Center 1.3]
- Restreindre les mises à jour des tickets RH à partir d’e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Limiter la durée de vie de la session active de l’interface utilisateur [nouveau dans Security Center 1.3]
- Appliquer la politique de référent sécurisé [Nouveau dans Security Center 1.3]

Paramètres de sécurisation renforcée mis à jour

Les paramètres de sécurisation renforcée mis à jour sont répartis pour chaque version de base de référence.

Paramètres de sécurisation renforcée mis à jour pour la version de base de référence 6.0

Certains paramètres de sécurisation renforcée ont été mis à jour avec la publication de la version de base de référence 6.0 du Centre de sécurité.

Documentation	Mises à jour
Empêcher l'accès non authentifié au client Web incorporé de l'agent virtuel	• Nouvelle description courte : Empêcher l’accès non authentifié au client Web intégré de l’Agent virtuel • Ancienne description courte :Client Web intégré de l’agent virtuel exposé publiquement sn_va_web_client_app_embed
Empêcher la création d’ACL vide [nouveau dans le centre de sécurité 2.0]	Règle : Script : le script a été mis à jour pour améliorer la précision de détection.
Activer les ACL pour une requête codée dans le widget de liste simple [nouveau dans Centre de sécurité 2.0]	• Score CVSS (nouveau) : 4,3 • Score CVSS (ancien) : 5,3

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Nettoyer tous les champs HTML traduits [nouveau dans Security Center 2.0]	• Score CVSS (nouveau) : 4,6 • Score CVSS (ancien) : 8,8
Activer l'assainisseur HTML [mis à jour dans Centre de sécurité 1.3]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mis à jour dans Centre de sécurité 1.3]	• Score CVSS (nouveau) : 5,9 • Score CVSS (ancien) : 7,1
Restreindre l'accès à l'API de script GlideSystemUserSession [Mise à jour dans Centre de sécurité 1.3 et 2.0]	• Rattrapage (nouveau) : assurez-vous que la propriété *glide.sandbox.usersession.allow_unsanitized_mess* est définie sur **false**. S'il n'existe aucun enregistrement de propriété système [sys_properties] pour cette propriété, créez-en un. • Rattrapage (ancien) : assurez-vous que la propriété *glide.sandbox.usersession.allow_unsanitized_mess* est définie sur **false**.
Interdire le clonage cible [Nouveau dans Security Center 1.3]	• Description (nouveau) : si *glide.db.clone.allow_clone_target* la valeur n'est pas définie sur la valeur conseillée, **faux**, l'instance peut être utilisée comme cible de clone ou comme enregistrement qui spécifie l'URL d'instance et les informations d'identification utilisées pour le clonage. On parle de clone système lorsque tout ce qui se trouve dans une base de données est copié d'une instance à une autre. Il s'agit d'un risque de sécurité, car la base de données d'instance peut être écrasée lors du processus de clonage, entraînant une perte de données et un manque d'intégrité des données. En guise de correction, assurez-vous que *glide.db.clone.allow_clone_target* est défini sur **faux**. Ne pas définir cette propriété sur la valeur recommandée faux permet à l'instance d'être utilisée comme cible du clone. Il s'agit d'un risque pour la sécurité, car la base de données d'instance peut être écrasée lors du processus de clonage. • Description (ancienne) : si *glide.db.clone.allow_clone_target* la propriété n'est pas définie sur la valeur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	conseillée, **faux**, l'instance peut être utilisée comme cible de clone. Cela risque que la base de données d'instance soit écrasée par un processus de clonage, entraînant une perte d'intégrité et de disponibilité.
Restreindre les paramètres OAuth au corps POST [nouveau dans Security Center 1.3]	• Score CVSS (nouveau) : 4,2 • Score CVSS (ancien) : 7,4
Appliquer la vérification de la liste d'autorisations d'URL [Mis à jour dans le Centre de sécurité 1.3, 1.5 et 2.0]	• Description (nouveau) : si `glide.security.url.whitelist.strict_check` n'est pas défini sur la valeur recommandée **Vrai** , toutes les URL externes sont autorisées à être redirigées lorsque `glide.security.url.whitelist` ce champ est vide. S'il `glide.security.url.whitelist` n'est pas vide, seules les URL externes de la liste d'inclusion sont autorisées. Ainsi, la définition `glide.security.url.whitelist.strict_check` sur vrai OU la garantie `glide.security.url.whitelist` est définie sur une valeur non vide avec les URL externes autorisées laisse l'instance dans un état sécurisé. Si toutes les URL externes sont autorisées à être redirigées, cela pourrait permettre à un attaquant de rediriger un utilisateur vers un site Web malveillant. • Description (ancienne) : si `glide.security.url.whitelist.strict_check` elle n'est pas définie sur la valeur conseillée **Vrai** et si `glide.security.url.whitelist` elle n'est pas définie sur l'URL approuvée par une organisation, toutes les URL externes sont autorisées à être redirigées. Cela pourrait permettre à un attaquant de rediriger un utilisateur vers un site Web malveillant. • Score CVSS (nouveau) : 6,3 • Score CVSS (ancien) : 8,3
Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mis à jour dans Centre de sécurité 1.3]	• Si la propriété système **glide.stax.whitelist_enabled** n'existe pas dans la table Propriétés système

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	[sys_properties], ou si elle n'est pas définie sur la valeur conseillée **true**, toutes les entités externes sont autorisées lorsque la propriété système **glide.stax.allow_entity_resolution** est définie sur la valeur **true**. Si les personnalisations ne nécessitent pas l'expansion de l'entité, utilisez la propriété système **glide.stax.allow_entity_resolution** pour désactiver l'expansion de l'entité externe. Le code XML termine l'analyse, mais n'inclut aucune entité interne ou externe. ◦ Si vous définissez **glide.stax.allow_entity_resolution** sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve du paramètre de la propriété **glide.stax.whitelist_enabled** . ◦ Si vous définissez glide.stax.allow_entity_resolution sur **faux**, toute la résolution et **l'expansion de l'entité** sont bloquées. Pour en savoir plus sur cette propriété, reportez-vous à la section Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5]. Lorsque **glide.stax.whitelist_enabled** est défini sur **vrai**, définissez une liste de FQDN délimités par des virgules dans la propriété **glide.xml.entity.whitelist** , qui sont les seules URL pouvant être atteintes à l'aide de la propriété de traitement d'entité XML. Pour en savoir plus, consultez Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]. Les attaquants peuvent utiliser cette vulnérabilité pour étendre les données de manière exponentielle dans une attaque d'expansion d'entités externes (XXE), consommant rapidement toutes les ressources système. • Description (ancienne) : si *glide.stax.whitelist_enabled* la valeur n'est pas définie sur la valeur conseillée **Vrai**, toutes les entités externes sont autorisées. Cela pourrait entraîner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	des attaques par extension d'entités externes (XXE). • Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]	• Protégez-vous contre les attaques XXE en utilisant une liste d'autorisation pour empêcher les attaquants d'inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait entraîner des attaques supplémentaires utilisant la relation de confiance du serveur avec d'autres entités. Ajoutez `http://java.sun.com/j2ee/dtds/` à la valeur de la propriété système **glide.xml.entity.whitelist** , puis définissez la propriété système **glide.xml.entity.whitelist.enabled** sur **true**. Des valeurs autres que `http://java.sun.com/j2ee/dtds/` peuvent être incluses dans la propriété **glide.xml.entity.whitelist** , mais ne sont pas nécessaires pour l'état de la plateforme prête à l'emploi. Examinez toutes les valeurs supplémentaires pour déterminer si elles sont sûres. **⚠ Avertissement :** Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible. • Description (ancienne) : si « glide.xml.entity.whitelist » n'est pas défini sur la valeur recommandée « http://java.sun.com/j2ee/dtds/ » et que « glide.xml.entity.whitelist.enabled » n'est pas défini sur « vrai », une entité externe malveillante peut être autorisée, ce qui pourrait entraîner une attaque XXE. Un attaquant peut utiliser la DTD pour inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait entraîner des attaques supplémentaires utilisant la relation de confiance du serveur avec d'autres entités. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Restreindre les domaines de messagerie pour l'inscription des utilisateurs externes [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Valider le type MIME de fichier dans AttachmentCreator SOAP Web Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Assurez-vous que les types MIME sont validés pour les pièces jointes afin d'empêcher le chargement de fichiers dangereux sur votre instance en utilisant des extensions de fichier incorrectes. Définissez la propriété système **glide.attachment.enforce_security_validation** sur **true**. Lorsque la valeur est définie sur **vrai**, les fichiers sont chargés avec l'extension de type de fichier correcte. • Description (ancienne) : si « glide.attachment.enforce_security_validation » n'est pas défini sur la valeur recommandée « vrai », il n'y aura aucune validation pour les pièces jointes de type MIME et des fichiers dangereux pourraient être téléchargés sur le système en utilisant des extensions de fichier incorrectes. Lorsque cette propriété est définie sur « vrai », les fichiers sont chargés avec l'extension de type de fichier correcte. Une bonne pratique de sécurité consiste à valider les chargements de fichiers au moins avec la validation de type MIME. • Score CVSS (nouveau) : 6,7 • Score CVSS (ancien) : 7,5
Définir les adresses IP internes autorisées ServiceNow [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Description (nouveau) Empêchez l'exposition inutile de l'accès à l'instance à un groupe plus large de personnes à l'aide des propriétés système **glide.ip.authenticate.strict** et **glide.ip.authenticate.allow.secured** . Lorsque la propriété système **glide.ip.authenticate.strict** est définie sur **vrai**, le personnel et les systèmes internes ServiceNow ne peuvent établir des connexions entrantes vers votre instance qu'à partir des plages IP essentielles. Cela limite ServiceNow la visibilité de l'infrastructure interne essentielle sur votre instance et empêche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	l'accès par un personnel plus large tel que le personnel de ServiceNow support et de vente via les réseaux de l'entreprise. La propriété système **glide.ip.authenticate.allow.secured** accorde des connexions entrantes internes ServiceNow , y compris un accès authentifié régulier et des pages de diagnostic non authentifiées. Si la valeur n'est pas définie sur **vrai**, une plage d'adresses IP interne plus large ServiceNow définie dans la propriété **glide.ip.authenticate.allow** est utilisée pour accorder ces connexions entrantes internes ServiceNow . Assurez-vous que la propriété système **glide.ip.authenticate.allow.secured** contient uniquement des valeurs fiables et que la propriété **glide.ip.authenticate.strict** est définie sur **vrai**. • Description (ancienne) : si « glide.ip.authenticate.strict » est définie sur « vrai », le personnel et les systèmes internes de ServiceNow ne peuvent établir des connexions entrantes vers l'instance qu'à partir des plages IP essentielles. Cela limite la visibilité de ServiceNow sur l'instance pour l'infrastructure interne essentielle et empêche l'accès par un personnel ServiceNow plus large, comme le personnel de support et de vente, via les réseaux de l'entreprise. Lorsqu'elle est définie sur « vrai », la propriété « glide.ip.authenticate.allow » est utilisée pour accorder les connexions entrantes ServiceNow internes. Si elle n'est pas définie sur « vrai », une plage d'adresses IP internes ServiceNow plus large, telle que définie dans « glide.ip.authenticate.allow », est utilisée pour accorder les connexions entrantes ServiceNow internes.
Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5]	• Description (Nouveau) : Désactivez l'expansion de l'entité sur votre instance pour la sécuriser contre les attaques telles que la capacité à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	lire des fichiers système et le déni de service. Utilisez la propriété système pour interdire le développement des entités XML lors de l'analyse par l'analyseur de diffusion (XMLDocument2). Définissez la propriété système **glide.stax.allow_entity_resolution** sur **faux** pour désactiver l'expansion de l'entité sur votre instance. Si cette propriété n'apparaît pas dans la table Propriétés système [sys_properties], la valeur par défaut est **vrai**. Créez l'enregistrement de propriété et définissez la valeur sur **faux** pour modifier sa valeur. • Description (ancienne) : si « glide.stax.allow_entity_resolution » n'est pas défini sur la valeur recommandée « Faux », cette propriété permet aux entités XML d'être développées lors de l'analyse par l'analyseur de diffusion en continu (XMLDocument2). L'extension de l'entité XML peut entraîner des attaques telles que la capacité à lire des fichiers système et le déni de service. • Rattrapage (nouveau) : assurez-vous que la propriété *glide.stax.allow_entity_resolution* existe dans la table sys_properties et qu'elle est définie sur **false**. Si la propriété n'apparaît pas dans la liste des sys_properties, la valeur par défaut est **vrai**. • Rattrapage (ancien) : assurez-vous que la propriété « glide.stax.allow_entity_resolution » est définie sur « faux ».
Refuser par défaut en cas d'ACL vides [Mis à jour dans Centre de sécurité 1.3]	• Description (Nouveau) : Empêchez le gestionnaire de sécurité hérité de votre instance d'autoriser l'accès aux ressources lorsqu'aucune ACL n'est définie pour cette ressource, ou s'il n'existe que des ACL au niveau de la table de caractères génériques (par exemple, incident.*). Lorsque l'accès est autorisé par défaut, tout ce qui n'a pas d'ACL explicites définies est susceptible d'être manipulé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Définissez la valeur de la propriété système **glide.sm.default_mode** sur **refuser** pour interdire l'accès lorsqu'il n'y a pas de règles ACL définies ou qu'il n'y a que des ACL au niveau de la table de caractères génériques. • Description (ancienne) : si « glide.sm.default_mode » n'est pas défini sur la valeur recommandée « refuser », le gestionnaire de sécurité hérité de l'instance autorise l'accès à une ressource alors qu'aucun ACL n'est défini pour cette ressource ; ou uniquement des ACL au niveau de la table de caractères génériques. Si cette option est définie sur « autoriser », tout ce qui n'a pas d'ACL explicite est susceptible d'être manipulé. • Score CVSS (nouveau) : 6,3 • Score CVSS (ancien) : 8,8 • Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Restreindre l'accès non authentifié aux pièces jointes	• Description (Nouveau) : Sécurisez les images sur votre instance pour éviter toute fuite d'informations sensibles. Les images de votre instance sont accessibles via des URL qui se terminent par .iix. Définissez la propriété système **glide.image_provider.security_enabled** sur **vrai** pour empêcher l'accès à vos images via ces URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Remarque : Cette propriété n'est pas respectée pour les images de la table des pièces jointes si la table d'origine est l'une des suivantes : ○ Papeterie [sysevent_email_style] ○ Sections de page d'accueil [sys_home] ○ Propriétés système [sys_properties] La restriction doit être appliquée aux utilisateurs non authentifiés, car certaines pièces jointes peuvent contenir des informations sensibles. • Description (ancienne) : si « glide.image_provider.security_enabled » n'est pas défini sur la valeur recommandée « Vrai », toutes les images sont accessibles via des URL se terminant par « .iix ». Cela permettrait un accès non authentifié aux images conduisant à une fuite d'informations sensibles.
Désactiver le code HTML intégré [Mis à jour dans Centre de sécurité 1.3]	• Description (Nouveau) : Désactiver la prise en charge de l'affichage du code HTML incorporé à l'aide de la balise `[code]`. Cette balise permet au HTML rendu de s'afficher dans les champs de journal et peut entraîner des attaques de script de site à site (XSS). Ces attaques peuvent permettre à des scripts étrangers de s'exécuter sur une session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent utiliser ces scripts pour voler des informations de session et des données sensibles. Le langage HTML n'a pas été conçu pour séparer le script du formatage, donc permettre le HTML contrôlé par l'utilisateur dans n'importe quel système comporte un risque inhérent. Définir la **glide.ui.security.codetag.allow_script** sur **faux** est conforme et réduit considérablement ce risque, mais un petit risque demeure. Il désactive uniquement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	la partie script d'une balise de `code` et s'appuie sur le nettoyage de toutes les conventions connues du script dans le HTML. Définissez la propriété système **glide.ui.security.allow_codetag** sur **false** pour interdire complètement aux champs et formulaires journaux d'afficher du contenu HTML rendu. Il ServiceNow AI Platform atténue de nombreuses attaques par injection et cross-site en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire/soumettre d'entrées au format HTML pour les champs journal. Mais les champs journaux peuvent rendre le texte entouré de balises de code en HTML. ○ Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur `vrai`, les utilisateurs malveillants peuvent écrire du code JS HTML nuisible qui peut être exécuté sur un navigateur client différent après le rendu des champs de journal. ○ Définissez cette propriété sur `faux` afin que les administrateurs puissent empêcher les champs de journal de rendre le code HTML en désactivant la prise en charge de la balise `[code]`. • Description (ancienne) : désactive la prise en charge de l'incorporation du code HTML créé à l'aide de la balise [code]. Si « glide.ui.security.allow_codetag » n'est pas défini sur la valeur « faux », le HTML affiché dans les champs et formulaires de journal n'est pas affiché. Définir « glide.ui.security.allow_codetag » sur « vrai » avec affichage du code HTML intégré avec peut entraîner des attaques de script de site à site (XSS).
Activer les contrôles de la politique de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Activer la notation et le filtrage d'e-mail indésirable [Mis à jour dans Centre de sécurité 1.3]	• Nom de configuration technique (nouveau) : com.glide.email_filter,glide.email.read.active • Nom de la configuration technique (ancien) : com.glide.email_filter • Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Formules Excel d'échappement [Mis à jour dans Centre de sécurité 1.3]	• Description (Nouveau) : Empêchez l'exécution de formules potentiellement malveillantes dans des programmes tels qu'Excel après l'exportation et l'ouverture du fichier en échappant les formules dans ces fichiers. L'injection Excel se produit lorsque les sites Web intègrent des entrées non approuvées dans des fichiers Excel. Lorsque vous utilisez une application de feuille de calcul telle que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les cellules commençant par +, -, = ou @ sont interprétées comme une formule à moins d'être correctement échappées. Les formules malveillantes présentent un risque même lorsque la feuille de calcul ne contient aucune information sensible, car elles peuvent être utilisées pour compromettre l'ordinateur du spectateur par l'exécution de code. Définissez la propriété système **glide.export.escape_formulas** sur **vrai** pour échapper l'exécution de ces formules. • Description (ancienne) : Définir la propriété « glide.export.escape_formulas » sur la valeur recommandée « vrai » empêche l'exécution de formules potentiellement malveillantes dans des programmes tels qu'Excel après l'exportation et l'ouverture du fichier. Les valeurs de cellule pour CSV, XLS et XLSX peuvent être interprétées comme des formules par les applications de feuille de calcul, sauf si elles sont correctement échappées, ce qui peut entraîner l'exécution de code malveillant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Score CVSS (nouveau) : 6,4 • Score CVSS (ancien) : 6,5
Restreindre les demandes JSONP aux URL approuvées [Mis à jour dans Centre de sécurité 1.3]	• Description (Nouveau) : Augmentez la sécurité sur votre instance en vous assurant que seules les URL approuvées pour le service de $http AngularJS peuvent autoriser/rejeter des demandes JSONP. Les demandes JSONP sont autorisées pour n'importe quelle URL si ces propriétés ne sont pas configurées et activées. Utilisez la valeur de la propriété système **angular.jsonp.inclusion_list.urls** pour définir une liste d'URL fiables et autorisées à cette fin. Définissez la valeur de la propriété système **angular.jsonp.inclusion_list.enabled** sur **true** pour limiter le JSONP autorisé aux URL répertoriées dans **angular.jsonp.inclusion_list.urls**. • Description (ancienne) : cette propriété spécifie des URL fiables pour le service de $http angularJS afin d'autoriser/ de rejeter des demandes JSONP. La propriété est nécessaire, car il s'agit d'un changement qui peut avoir des conséquences importantes pour les clients, ils ont donc besoin d'un moyen d'ajouter leurs URL de confiance. Si la propriété « angular.jsonp.inclusion_list.enabled » n'est pas définie sur la valeur conseillée « vrai », les demandes JSONP sont autorisées pour n'importe quelle URL
Activer le module d'extension du contrôle d'accès SNC [Mis à jour dans Centre de sécurité 1.3]	• Description (Nouveau) : Empêchez ServiceNow le personnel du service clientèle et de l'assistance d'accéder aux instances sans votre autorisation expresse en activant le module d'extension SNC Access Control (com.snc.snc_access_control). Bien que tous les accès à votre instance soient audités, vous préférez peut-être contrôler cet accès. Cette méthode d'accès est entièrement auditable et suivie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Remarque : D’autres membres du personnel d’exploitation autorisés ServiceNow , dans leur capacité à prendre en charge et à gérer le produit, sont tenus d’effectuer des actions administratives sur l’infrastructure sous-jacente. L’activation de ce module d’extension peut affecter les niveaux de service d’assistance et le SLA de disponibilité. La disponibilité du SLA est ensuite mesurée à partir du moment où le personnel de support est autorisé à accéder à votre instance. Activez le module d’extension SNC Access Control (com.snc.snc_access_control) pour restreindre l’accès à votre instance sans votre autorisation expresse. Pour en savoir plus sur cette fonctionnalité, reportez-vous à la section Contrôle d'accès ServiceNow. Pour plus d’informations sur l’activation, consultez Activer ServiceNow le contrôle d’accès • Description (ancienne) : Le module d’extension Contrôle d’accès SNC (com.snc.snc_access_control) empêche le personnel du service clientèle et de l’assistance d’accéder aux instances sans votre autorisation expresse. Toutefois, d’autres membres du personnel autorisé des opérations ServiceNow, en sa capacité à prendre en charge et à gérer le produit, sont nécessaires pour effectuer des actions administratives sur l’infrastructure sous-jacente. Cette infrastructure comprend des serveurs et des bases de données, entre autres composants de l’infrastructure qui composent la solution SaaS. Cette méthode d’accès est entièrement auditable et suivie. Ce module d’extension vous permet de restreindre l’accès à votre instance sans votre autorisation expresse, de sorte que cela peut affecter les niveaux de service d’assistance et le SLA de disponibilité. La disponibilité du SLA est ensuite mesurée à partir du moment où le personnel de support est autorisé à accéder à votre instance. • Rattrapage (nouveau) : assurez-vous que le module d’extension « com.snc.snc_access_control » est activé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Lisez la documentation sur l'activation à https://www.servicenow.com/docs/csh?topicname=t_ActivateSNCAccessControl.html&version=latest. • Rattrapage (ancien) : assurez-vous que le module d'extension « com.snc.snc_access_control » est activé. • Score CVSS (nouveau) : 3,3 • Score CVSS (ancien) : 8,2
Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion [Mis à jour dans Centre de sécurité 1.3]	• Nom de la configuration technique (nouvelle) : glide.user.unlock_timeout_in_mins, sysevent_script_action • Nom de la configuration technique (ancien) : glide.user.unlock_timeout_in_mins • Description (Nouveau) : Protégez votre instance contre les attaques par force brute en définissant une période pendant laquelle un utilisateur ne peut pas tenter de se connecter après avoir été verrouillé. La propriété système **glide.user.unlock_timeout_in_mins** déverrouille le compte d'utilisateur après la période spécifiée dans sa valeur. Si aucune valeur n'est spécifiée, votre instance déverrouille le compte d'utilisateur après la période par défaut de 15 minutes. • Description (ancienne) : si « glide.user.unlock_timeout_in_mins » n'est pas défini sur la valeur recommandée de « 15 », il peut être plus facile d'effectuer une attaque par force brute des comptes dans un délai plus rapide. Cette propriété déverrouille le compte d'utilisateur après la période spécifiée pour la propriété glide.user.unlock_timeout_in_mins. Si aucune valeur n'est spécifiée, le système déverrouille le compte d'utilisateur après la période par défaut de 15 minutes. • Rattrapage (nouveau) : Définissez la valeur de la propriété système **glide.user.unlock_timeout_in_mins** sur un minimum de **15**. Si **glide.user.unlock_timeout_in_mins n'existe**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	pas, la durée de verrouillage par défaut est fixée à 15 minutes. Assurez-vous que l'action **des scripts Vérification du verrouillage de l'utilisateur SNC avec déverrouillage automatique** (qui se trouve dans la table Action des scripts [sysevent_script_action]) est présente et active. L'action **de script Vérification de verrouillage de l'utilisateur SNC avec déverrouillage automatique** est installée avec le module d'extension Paramètres de sécurité élevée (com.glide.high_security). • Rattrapage (ancien) : assurez-vous que la propriété « glide.user.unlock_timeout_in_mins » est définie sur « 15 » ou plus. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Restreindre l'accès aux module d'extension de plages d'adresses IP spécifiques [Mis à jour dans Centre de sécurité 1.3]	• Nom de configuration technique (nouveau) : com.snc.ipauthenticator,ip_access • Nom de la configuration technique (ancien) : com.snc.ipauthenticator
Restreindre l'accès aux e-mails dont la table cible est vide	• Score CVSS (nouveau) : 6,5 • Score CVSS (ancien) : 5,4
Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Score CVSS (nouveau) : 6,4 • Score CVSS (ancien) : 8
Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nom de la configuration technique (nouveau) : glide.authenticate.multissov2_feature.enabled • Nom de configuration technique (ancien) : glide.authenticate.multisso.enabled,glide.authenticate.mult • Description (Nouveau) : Si le module d'extension Multi SSO est activé sur une instance, réduisez les vulnérabilités de sécurité en confirmant que la version v2 est activée. La dernière version renforce la sécurité et dispose de plus de fonctionnalités, telles que la prise en charge du chiffrement d'assertion et la déconnexion unique (SLO) initiée par IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Si la dernière version n'est pas activée, les nouvelles fonctionnalités de sécurité ne peuvent pas être utilisées et l'instance risque d'utiliser un module d'extension déconseillé. Suivez les étapes de KB0756504 pour effectuer une mise à niveau vers la dernière version. Ce processus comprend la vérification et la migration de tous les changements liés à la personnalisation, puis la mise à niveau de la version. Lorsque vous avez terminé, la propriété système **glide.authenticate.multissov2_feature.enabled** est automatiquement définie **sur vrai**. • Description (ancienne) : si le module d'extension Multi SSO est activé sur une instance, la version v2 doit être activée. Les versions antérieures à MultiSSOv2, y compris SAML 1.1 et SAML 2.0, ne suivent pas les bonnes pratiques et utilisent des versions de bibliothèque opensaml avec des CVE connus. Si les CVE connus étaient exploitables dans des bibliothèques openaml obsolètes, cela pourrait permettre à l'attaquant de falsifier des messages et de contourner l'authentification par le biais d'attaques par encapsulation de signature XML, d'emprunter l'identité d'entités ou de permettre à des attaquants d'homme de milieu d'obtenir un accès non autorisé à la plateforme. • Score CVSS (nouveau) : 0 • Score CVSS (ancien) : 7,1
Empêcher les utilisateurs inactifs de se connecter [nouveau dans le centre de sécurité 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Activer le journal d'audit MID [nouveau dans Security Center 1.3 et mis à jour dans 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Assurez-vous que les ACL de table d'archivage sont vérifiées [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Définir les rôles d'exception de délai d'expiration de session active [nouveau dans Security Center 1.3]	• Score CVSS (nouveau) : 6,4 • Score CVSS (ancien) : 7,1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Limiter la taille du corps de la réponse HTTP [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Description (Nouveau) : Empêchez les exceptions OutOfMemoryExceptions qui peuvent résulter d'un corps de réponse de demande trop volumineux à l'aide des propriétés système **glide.http.response.get_body.limit.enabled** et **glide.http.response.get_body.limit** . Ces exceptions peuvent provoquer des attaques par déni de service (DOS) ainsi que d'autres problèmes susceptibles d'aider les attaquants à compromettre une instance. Si vous ne définissez pas ces propriétés sur les valeurs recommandées, votre instance peut être vulnérable aux exceptions OutOfMemoryExceptions et aux attaques par déni de service. Pour protéger votre instance contre ces vulnérabilités de sécurité : ◦ Définissez la propriété système **glide.http.response.get_body.limit.enabled** sur **true**. ◦ Assurez-vous que la propriété système **glide.http.response.get_body.limit** est définie sur 524 288 000 mégaoctets (500 Mo). • Description (ancienne) : Les propriétés glide.http.response.get_body.limit.enabled et glide.http.response.get_body.limit ont été introduites pour permettre une nouvelle fonctionnalité qui empêche les exceptions de mémoire insuffisante d'être levées lorsque le corps d'une réponse aux demandes est trop volumineux. Les exceptions de mémoire insuffisante peuvent entraîner des attaques par déni de service ainsi que d'autres problèmes susceptibles d'aider les attaquants à compromettre une instance. • Score CVSS (nouveau) : 3,1 • Score CVSS (ancien) : 6,4
Limiter la durée de vie de la session active de l'interface utilisateur [nouveau dans Security Center 1.3]	• Description (Nouveau) : Réduisez la portée des incidents de sécurité potentiels en diminuant la durée de vie des sessions HTTP actives. La propriété système

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	glide.ui.active.session.life_span applique une durée de vie maximale sur les sessions HTTP actives, quel que soit le délai d'expiration inactif. Des durées de vie maximales plus longues peuvent permettre à un attaquant d'utiliser une session volée plus longtemps, augmentant ainsi la portée d'un incident de sécurité. La valeur par défaut de **0** désactive le délai d'expiration des sessions actives Définissez le **glide.ui.active.session.life_span** sur une valeur comprise entre 1 et 720. Cette valeur représente la durée en minutes pendant laquelle les sessions HTTP peuvent rester actives. • Description (ancienne) : cette configuration applique la durée de vie maximale sur les sessions HTTP d'invités actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes et la valeur de zéro désactive l'expiration des sessions actives. Une durée de vie maximale plus longue pourrait permettre à un attaquant de persister plus longtemps dans une session volée, augmentant ainsi la portée d'un incident de sécurité. Cette propriété particulière est limitée à l'expiration de session d'interface utilisateur.

Paramètres de sécurisation renforcée mis à jour pour la version de base de référence 5.0

Certains paramètres de sécurisation renforcée ont été mis à jour avec la publication de la version de base de référence 5.0 du Centre de sécurité.

La version 5 de base de référence inclut plusieurs mises à jour des brèves descriptions pour des raisons de style et de cohérence entre les enregistrements. En outre, de nombreux scripts liés aux propriétés ont été mis à jour pour améliorer la précision des valeurs par défaut dans les cas où la propriété a été supprimée de la table sys_property.

Documentation	Mises à jour
Exiger une autorisation pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.basicauth.required.soap` Glide existe et qu'elle est définie sur la valeur vrai. Vous pouvez également configurer l'instance pour la sécurité WS en définissant la propriété glide.soap.require_ws_security sur true et en suivant la documentation du produit

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	pour configurer les profils de sécurité WS. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.soap` est définie sur la valeur vrai. Vous pouvez également configurer l'instance pour la sécurité WS en définissant la propriété `glide.soap.require_ws_security` sur vrai et en suivant la documentation du produit pour configurer les profils de sécurité WS.
Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]	• Nouvelle correction : assurez-vous que la propriété `com.glide.communications.httpclient.ocsp_allow_` existe et qu'elle est définie sur false. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `com.glide.communications.httpclient.ocsp_allow_` est définie sur false.
Désactiver l'URL du contenu externe [Mis à jour dans Centre de sécurité 2.0]	• Nouveau rattrapage : assurez-vous que la propriété `glide.ui.url.external.content` Glide existe et qu'elle est définie sur la valeur faux. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.ui.url.external.content` est définie sur false. • Nouveau score CVSS : 7,2 • Ancien score CVSS : 8,1 • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]	• Nouveau rattrapage : assurez-vous que la propriété `glide.xml.entity.whitelist` Glide existe et est définie sur « http://java.sun.com/j2ee/dtds/ » et que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.xml.entity.whitelist.enabled` Glide existe et est définie sur la valeur vrai. Si les propriétés n'apparaissent pas dans la table sys_properties, ajoutez de nouveaux enregistrements. • Ancien rattrapage : assurez-vous que la propriété `glide.xml.entity.whitelist` est définie sur « http://java.sun.com/j2ee/dtds/ » et que la propriété `glide.xml.entity.whitelist.enabled` est définie sur vrai.
Désactiver les rapports publiés non authentifiés [Mis à jour dans Centre de sécurité 2.0]	• Nouveau rattrapage : assurez-vous que la propriété `glide.report.published_reports.enabled` Glide existe et qu'elle est définie sur la valeur faux. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.report.published_reports.enabled` est définie sur false.
Activer les contrôles de la politique de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.enable.password_policy` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.enable.password_policy` est définie sur vrai.
Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts [mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.xmlutil.max_entity_expansion` est définie sur 3 000 ou moins. Si l'instance est sur Washington ou une version ultérieure, la valeur implicite par défaut est 3 000 si l'enregistrement sys_properties n'existe pas. Si l'instance n'est pas sur Washington ou une version ultérieure, il est recommandé à l'administrateur de l'instance de créer un enregistrement de sys_properties avec le nom

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.xmlutil.max_entity_expansion` et la valeur 3 000. • Ancien rattrapage : assurez-vous que la propriété `glide.xmlutil.max_entity_expansion` est définie sur 3 000 ou moins.
Désactiver les connexions SSLv2/SSLv3 sortantes [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle correction : assurez-vous que la propriété `glide.outbound.sslv3.disabled` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.outbound.sslv3.disabled` est définie sur vrai. **Important :** La valeur de la `glide.outbound.sslv3.disabled` propriété est un remplacement sûr et ne peut pas être modifiée une fois modifiée.
Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle description brève : Désactiver le comportement hérité de clôture du champ d'application GlideRecord • Ancienne description brève : Activer le comportement hérité de clôture du champ d'application GlideRecord
Restreindre les types MIME chargés [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.security.file.mime_type.validation` existe et qu'elle est définie sur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.security.file.mime_type.validation` est définie sur vrai.
Activer la protection de l'interpolation Jelly JS pour les expressions imbriquées [Mis à jour dans Centre de sécurité 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.ui.jelly.js_interpolation.protect_nested_e` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété *glide.ui.jelly.js_interpolation.protect_nested_e* est définie sur vrai.
Activer SSL dans l'authentification LDAP [Mis à jour dans Centre de sécurité 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer UserCookie version 3.1 [Mis à jour dans Centre de sécurité 2.0]	• Nouvelle description : UserCookie v3 est généré uniquement lorsque la propriété *glide.ui.secure.cookies.use_kmf is disabled*. UserCookie v3 n'est pas sécurisé en raison du stockage de clé secrète pour HMAC dans le code source et identique pour tous les clients. Cela peut permettre à des acteurs malveillants d'utiliser cette clé secrète unique pour tenter de détourner des sessions utilisateurs. En définissant la propriété *glide.ui.secure.cookies.use_kmf* sur vrai, UserCookie v3.1 sera utilisé et la clé secrète sera stockée dans un stockage de sécurité tel que KMF. • Ancienne description : UserCookie v3 est généré uniquement lorsque la propriété *glide.ui.secure.cookies.use_kmf* est désactivée. UserCookie v3 n'est pas sécurisé en raison du stockage de clé secrète pour HMAC dans le code source et identique pour tous les clients. Cela peut permettre à des acteurs malveillants d'utiliser cette clé secrète unique pour tenter de détourner des sessions utilisateurs. • Nouvelle correction : assurez-vous que la propriété *glide.ui.secure.cookies.use_kmf* existe et qu'elle est définie sur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété *glide.ui.secure.cookies.use_kmf* est définie sur vrai. Ce qui signifie que UserCookie v3.1 sera utilisé et que la clé secrète sera stockée dans un stockage de sécurité tel que KMF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Définir la durée de vie de l'OTP pour la réinitialisation du mot de passe à 1 heure [Mis à jour dans Centre de sécurité 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Enregistrer l'emprunt d'identité d'un utilisateur [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.sys.log_impersonation` existe et qu'elle est définie sur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la propriété `glide.sys.log_impersonation` est définie sur vrai.
Instanciateurs de connexions JMS requis [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
S'assurer que la création/la suppression des tableaux de bord nécessite une vérification d'accès [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.processors.check_access_before_process` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : assurez-vous que la valeur de `glide.processors.check_access_before_process` a toujours la valeur vrai.
Invalider de manière proactive les sessions inactives [nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle correction : assurez-vous que la propriété `glide.active.session.timeout.invalidate.session` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement. • Ancien rattrapage : définissez la propriété `glide.active.session.timeout.invalidate.session` Glide sur vrai.
Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
[Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]	
Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description : si la propriété *glide.ui.attachment.force_download_all_mime_type* est définie sur vrai, elle *glide.ui.attachment.download_mime_types* est alors remplacée afin que tous les types MIME soient téléchargés plutôt qu'affichés par le navigateur. Par exemple, le téléchargement de texte/html force un fichier HTML à être téléchargé sur le client en tant que fichier plutôt que d'être affiché en ligne dans le navigateur, empêchant ainsi une attaque XSS. XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué. • Ancienne description : si la propriété *glide.ui.attachment.force_download_all_mime_type* n'est pas définie sur vrai, la *glide.ui.attachment.download_mime_types* propriété est alors remplacée afin que tous les types MIME soient téléchargés plutôt qu'affichés par le navigateur. Par exemple, le téléchargement de texte/html force un fichier HTML à être téléchargé sur le client en tant que fichier plutôt que d'être affiché en ligne dans le navigateur, empêchant ainsi une attaque XSS. La possibilité d'avoir un XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué. • Nouvelle correction : assurez-vous que la propriété *glide.ui.attachment.force_download_all_mime_type* est définie sur true. Si la propriété n'existe pas dans la table sys_properties, la valeur par défaut est faux. • Ancien rattrapage : assurez-vous que la propriété *glide.ui.attachment.force_download_all_mime_type* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Définir les types MIME téléchargeables restreints [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver le téléchargement des fichiers infectés [Mis à jour dans Security Center 1.5 et 2.0]	• Nouvelle description : lorsque la propriété `com.glide.snap.infected_download_allowed` est définie sur vrai, les utilisateurs peuvent toujours télécharger des pièces jointes non analysées au cas où le service antivirus serait en panne ou inaccessible. Cela signifie qu'il est possible qu'un utilisateur télécharge un fichier malveillant et risque d'infecter le bureau de l'utilisateur (au cas où il n'y aurait pas d'autre protection de point de terminaison sur l'appareil). • Ancienne description : si `com.glide.snap.infected_download_allowed` n'est pas défini sur la valeur recommandée Faux, il est possible de télécharger un fichier malveillant qui n'a pas été analysé, ce qui entraîne un risque d'infection du bureau de l'utilisateur. • Nouvelle correction : assurez-vous que la propriété `com.glide.snap.infected_download_allowed` est définie sur false. • Ancien rattrapage : assurez-vous que la propriété `com.glide.snap.infected_download_allowed` est définie sur Faux.
Restreindre l'accès à l'API de script GlideSystemUserSession [Mise à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description : `gs.addErrorMessageNoSanitizationMessaging()` et `gs.addInfoMessageNoSanitization()` sont utilisés dans l'environnement de script pour la journalisation et les notifications. Ces deux éléments sont disponibles dans le bac à sable si cette propriété n'est pas définie sur la valeur recommandée faux Le bac à sable est un environnement de script avec peu de privilèges disponible pour les utilisateurs non authentifiés et sans rôle. Ces deux méthodes peuvent être utilisées pour afficher une entrée non expurgée à un utilisateur. L'affichage d'une entrée non expurgée à l'utilisateur est dangereux, car l'entrée non expurgée peut contenir du code dangereux qui s'exécute dans le navigateur de l'utilisateur. Cela peut être utilisé pour les attaques XSS

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	réfléchies traditionnelles. Les attaques XSS réfléchies peuvent être utilisées dans plusieurs scénarios, y compris le détournement de session. • Ancienne description : la messagerie dans le bac à sable de scripting Glide est utilisée à des fins de journalisation. L'appel de cette fonction d'erreur non expurgée expose la plateforme à des attaques XSS réfléchies. Les attaques XSS peuvent permettre une escalade facile des privilèges en volant les cookies de session de quelqu'un. Si `glide.sandbox.usersession.allow_unsanitized_mess` n'est pas défini sur la valeur recommandée faux, les fonctions de messagerie d'erreurs non assainies `addErrorMessageNoSanitization` et `addInfoMessageNoSanitization` sont disponibles pour le script.
Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]	• Nouvelle description : lorsque la valeur est définie sur vrai, les règles/filtres de sn_query_rule table seront utilisés pour déterminer l'accès en lecture aux tables liées à Gestion des services sur site (commande de travaux et tâche de commande de travaux) à l'utilisateur connecté via les règles métier des requêtes et les ACL en lecture. Si la valeur est définie sur false, les enregistrements ne sont pas filtrés en fonction des règles de requête. Les règles métier des requêtes ajoutent des validations de sécurité supplémentaires. Plus précisément, cette propriété filtre les enregistrements d'agents, de qualificateurs et de répartiteurs en fonction du territoire qui leur est affecté ou de leur appartenance au territoire. Il est préférable de suivre le principe du moindre privilège lors de la lecture des documents. Lorsque cette propriété n'est pas définie sur vrai, il peut y avoir un risque accru d'exposition des données des tables Gestion des services sur site. • Ancienne description : lorsque la valeur est définie sur vrai, les règles/filtres de sn_query_rule table seront utilisés pour déterminer l'accès en lecture aux tables liées à Gestion des services sur site (commande de travaux et tâche de commande de travaux) à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	l'utilisateur connecté via les règles métier des requêtes et les ACL en lecture. Si la valeur est définie sur false, les enregistrements ne sont pas filtrés en fonction des règles de requête. Les règles métier des requêtes ajoutent des validations de sécurité supplémentaires. Plus précisément, cette propriété filtre les enregistrements d'agents, de qualificateurs et de répartiteurs en fonction du territoire qui leur est affecté ou de leur appartenance au territoire. Il est préférable de suivre le principe du moindre privilège lors de la lecture des documents.
Restreindre les domaines de messagerie pour l'inscription des utilisateurs externes [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description : la *sn_ext_usr_reg.allowed_email_domains* propriété définit les adresses e-mail autorisées à s'auto-enregistrer sur une instance ServiceNow. Le format doit être une liste séparée par des virgules de domaines d'e-mail acceptables, tels que domain1.com,domain2.com où les e-mails tels que example@domain2.com seront acceptés. S'il *sn_ext_usr_reg.allowed_email_domains* n'est pas défini avec une liste de domaines acceptables, les utilisateurs avec n'importe quelle adresse e-mail sont autorisés à enregistrer des comptes sur les instances. Si cette propriété n'est pas définie, les acteurs malveillants peuvent effectuer l'enregistrement à l'aide d'adresses e-mail de domaines indésirables pour obtenir un accès authentifié à l'instance. • Ancienne description : la *sn_ext_usr_reg.allowed_email_domains* propriété définit les adresses e-mail autorisées à s'auto-enregistrer sur une instance ServiceNow. S'il *sn_ext_usr_reg.allowed_email_domains* n'est pas défini avec une liste de domaines acceptables, les utilisateurs avec n'importe quelle adresse e-mail sont autorisés à enregistrer des comptes sur les instances. Si cette propriété n'est pas définie, les acteurs malveillants peuvent effectuer l'enregistrement à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	l'aide d'adresses e-mail de domaines indésirables pour obtenir un accès authentifié à l'instance.
Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description : cette propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de type « remontée pas à pas ». Si `glide.sys.domain.include_domain_condition_on_jo` cette propriété n'est pas définie sur la valeur recommandée vrai sur une instance utilisant Séparation de domaine, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique. L'instance peut avoir un impact fonctionnel modéré si les composants dépendent des requêtes interdomaines non sécurisées. Les instances doivent être testées dans des environnements de sous-production avant l'activation. • Ancienne description : cette propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de remontée pas à pas. Si `glide.sys.domain.include_domain_condition_on_jo` cette propriété n'est pas définie sur la valeur recommandée vrai sur une instance utilisant Séparation de domaine, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique.
Appliquer la vérification de la liste d'autorisations d'URL [Mis à jour dans le Centre de sécurité 1.3, 1.5 et 2.0]	• Nouveau rattrapage : assurez-vous que la propriété `glide.security.url.whitelist.strict_check` est définie sur vrai ou que la propriété `glide.security.url.whitelist` est définie sur une valeur. • Ancien rattrapage : assurez-vous que la propriété `glide.security.url.whitelist.strict_check`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	est définie sur « vrai » et que la propriété `glide.security.url.whitelist` est définie sur une valeur.
Définir l'utilisateur invité pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre l'accès au script en arrière-plan [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description : cette propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si `glide.script_processor.admin` elle n'est pas définie sur la valeur recommandée et par défaut administrateur, les utilisateurs ayant un rôle avec moins de privilèges seront en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela conduira à un contournement complet du système d'ACL permettant un accès complet aux tables. • Ancienne description : cette propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si `glide.script_processor.admin` elle n'est pas définie sur la valeur recommandée admin, security_admin ou maint, les utilisateurs ayant un rôle avec moins de privilèges seront en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela conduira à un contournement complet du système d'ACL permettant un accès complet aux tables. • Nouvelle correction : assurez-vous que la propriété `glide.script_processor.admin` est définie sur l'administrateur. Il s'agit de la valeur par défaut pour les instances. • Ancien rattrapage : assurez-vous que la propriété `glide.script_processor.admin` est définie sur le rôle d'administrateur, de security_admin ou de maintenance.
Vérifier la chaîne et le nom d'hôte des certificats [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]	• Nouvelle description : lorsque la propriété `com.glide.communications.httpclient.verify_hostn` Glide n'est pas définie sur la valeur sécurisée true, le nom d'hôte et la chaîne de certification présentés par les hôtes distants lors d'une connexion TLS initiée à partir de l'instance ServiceNow ne sont pas validés. Cela pourrait compromettre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	la sécurité de la connexion TLS et permettre des attaques de l'homme du milieu, où les communications entre deux parties sont interceptées. Cela peut entraîner la divulgation de données sensibles. • Ancienne description : si *com.glide.communications.httpclient.verify_hostn* la valeur n'est pas définie sur vrai, cela pourrait permettre des attaques de l'homme du milieu où les communications entre deux parties sont interceptées. La définition de cette propriété sur une valeur non sécurisée désactive le processus de vérification des certificats qui évalue toutes les certifications de la chaîne de certificats en vérifiant l'état de révocation. Définissez cette propriété sur vrai pour empêcher le client HTTP de se connecter à un nom d'hôte potentiellement dangereux.
Délai de verrouillage du contrôle pour les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : *Control Lockout Time for Invalid Password Reset Attempts* • Ancienne description brève : *Minimize Reset Password Request Max Attempts Window Duration* • Nouvelle description : la *password_reset.request.max_attempt_window* propriété définit le nombre de minutes pendant lesquelles un utilisateur doit patienter avant de réinitialiser ou de changer son mot de passe après avoir dépassé le nombre maximal de tentatives infructueuses défini avec le *password_reset.request.max_attempt property*. Un petit nombre de minutes pour la *password_reset.request.max_attempt_window* propriété augmente le risque d'attaque par force brute réussie d'un mot de passe, car un plus grand nombre de tentatives de réinitialisation du mot de passe peuvent être effectuées. La valeur par défaut de 1440 minutes est recommandée. • Ancienne description : si *password_reset.request.max_attempt_window* n'est pas défini sur la valeur recommandée de 1 440 ou moins, il est possible d'effectuer une attaque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	bruteforce du compte, car le compte ne sera pas verrouillé après un nombre maximal de tentatives d'authentification incorrectes. • Nouvelle correction : assurez-vous que la propriété *password_reset.request.max_attempt_window* est définie sur 1 440 ou plus. • Ancien rattrapage : assurez-vous que la propriété *password_reset.request.max_attempt_window* est définie sur 1 440 ou moins. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle description brève : *Disable GlideRecord Scope Fencing Legacy Behavior* • Ancienne description brève : *Enable GlideRecord Scope Fencing Legacy Behavior* • Nouvelle correction : définissez la propriété *glide.record.legacy_cross_scope_access_policy_in* Glide sur faux. Lorsqu'elle n'est pas présente dans la table sys_properties, la valeur par défaut est vrai. • Ancien rattrapage : définissez la propriété *glide.record.legacy_cross_scope_access_policy_in* Glide sur faux.
Limiter les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et mis à jour dans la version 2.0]	• Nouvelle description brève : *Limit Invalid Password Reset Attempts* • Ancienne description brève : *Minimize Reset Password Request Max Attempt Allowance*

Paramètres de sécurisation renforcée mis à jour pour la version de base de référence 4.0

Certains paramètres de sécurisation renforcée ont été mis à jour avec la sortie de la version de base de Centre de sécurité référence 4.0.

La version de base de référence 4.0 inclut plusieurs mises à jour des brèves descriptions pour le style et la cohérence entre les enregistrements. En outre, de nombreux scripts liés aux propriétés ont également été mis à jour afin d'améliorer la précision de la valeur par défaut pour les tickets où la propriété a été supprimée de la table sys_property.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Exiger une autorisation pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouveau nom de la configuration technique : `glide.basicauth.required.soap, glide.soap.require_ws_security` • Ancien nom de la configuration technique : `glide.basicauth.required.soap` • Nouvelle description : la propriété `glide.basicauth.required.soap` Glide contrôle si l'authentification de base est requise pour effectuer une demande SOAP à une instance. Si `glide.basicauth.required.soap` cette option n'est pas définie sur la valeur conseillée, vrai, les utilisateurs non authentifiés qui effectuent des opérations SOAP sont mappés à l'utilisateur soap.guest. Cela peut permettre à un utilisateur non authentifié d'effectuer des opérations sur l'instance comme s'il s'agissait d'un utilisateur connecté à l'instance. Il peut y avoir un impact supplémentaire si l'utilisateur défini dans `com.glide.soap.guest_user` se voit attribuer des rôles supplémentaires. • Ancienne description : la propriété `glide.basicauth.required.soap` Glide contrôle si une authentification est requise pour effectuer une demande SOAP à une instance. Si `glide.basicauth.required.soap` la valeur recommandée n'est pas définie sur vrai, l'authentification est désactivée pour les demandes SOAP sur l'instance. Il permet un accès non authentifié aux opérations de niveau administrateur ou de maintenance ; annulant ainsi les contrôles de sécurité au sein de l'instance. • Nouvelle correction : assurez-vous que la propriété `glide.basicauth.required.soap` est définie sur la valeur vrai. Vous pouvez également configurer l'instance pour la sécurité WS en définissant la propriété `glide.soap.require_ws_security` sur vrai et en suivant la documentation du produit pour configurer les profils de sécurité WS. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.soap` existe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	dans la table sys_properties et qu'elle est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Script Jelly d'échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : cette propriété échappe toutes les chaînes JS et HTML incluses avant qu'elles ne soient écrites dans le flux de sortie, empêchant ainsi plusieurs problèmes XSS de se produire. Si `glide.ui.escape_all_script` n'est pas défini sur la valeur recommandée true, l'échappement des scripts injectés dans Jelly est désactivé. Sans cette atténuation, la plateforme devient largement ouverte à une variété d'attaques par injection de script. Un attaquant pourrait exécuter des scripts Rhino arbitraires sur l'instance. • Ancienne description : La propriété suivante échappe à toutes les chaînes JS et HTML incluses dans <j :jelly> ... </j :jelly> avant qu'ils ne soient écrits dans le flux de sortie, ce qui évite que plusieurs problèmes XSS ne se produisent. Si `glide.ui.escape_all_script` n'est pas défini sur la valeur recommandée « vrai », l'échappement des scripts injectés dans Jelly est désactivé. Sans cette atténuation, la plateforme devient largement ouverte à une variété d'attaques par injection de script. Un attaquant pourrait exécuter des scripts Rhino arbitraires sur l'instance.
Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF • Ancienne description brève : Appliquer la validation stricte du jeton CSRF • Nouvelle description : cette propriété empêche les utilisateurs d'accepter un avertissement qui permet d'envoyer une demande potentiellement malveillante à l'instance. Cet avertissement s'affiche lorsqu'une requête POST échoue en raison d'un jeton anti-CSRF qui ne correspond pas et qui appartient à l'une des autres sessions actives de la victime. S'il

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.security.csrf.strict.validation.mode` n'est pas défini sur la valeur recommandée true, un attaquant peut formuler une attaque CSRF en utilisant un jeton anti-CSRF d'une autre session active appartenant à la victime. Une demande POST à une instance contient un jeton anti-CSRF dans sysparm_ck ou X-UserToken qui correspond à la session actuelle de l'utilisateur. Si le jeton anti-CSRF est plutôt lié à l'une des autres sessions actives de l'utilisateur, la demande POST renvoie une redirection 302 vers security_interceptor.do avec un bouton Continuer disponible pour l'utilisateur lorsque cette propriété est définie sur faux. Cliquer sur ce bouton soumet à nouveau la demande à l'instance, sauf qu'elle dispose désormais d'un jeton anti-CSRF valide. Lorsque cette propriété est définie sur vrai, la redirection 302 vers la page security_interceptor.do n'affiche pas de bouton Continuer et l'utilisateur n'est pas autorisé à soumettre à nouveau la demande. Une attaque CSRF réussie permettra à un attaquant d'effectuer efficacement n'importe quelle opération que la victime est capable d'effectuer. • Ancienne description : cette propriété active la validation stricte des jetons CSRF, ce qui empêche la réutilisation des jetons CSRF. Si `glide.security.csrf.strict.validation.mode` la valeur recommandée n'est pas définie sur vrai, les jetons CSRF peuvent être réutilisés, ce qui ouvre la porte à des attaques CSRF. • Nouveau score CVSS : 3,7 • Ancien score CVSS : 3,1
Exiger l'authentification sur le processeur HTTP de Gestion des événements [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]	• Nouvelle description brève : Exiger l'authentification sur le processeur HTTP de Gestion des événements • Ancienne description brève : Exiger l'authentification sur le processeur HTTP de Gestion des événements
Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]	• Nouvelle description : la contrefaçon de requête intersite (CSRF) est une attaque qui force les utilisateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	authentifiés à soumettre une demande à une application Web par rapport à laquelle ils sont actuellement authentifiés. Les attaques CSRF exploitent la confiance qu'une application Web accorde à un utilisateur authentifié. Cette propriété permet l'utilisation d'un jeton de sécurité pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite. Si `glide.security.use_csrf_token` la valeur recommandée n'est pas définie sur true, CSRF est possible. • Ancienne description : La contrefaçon de requête intersite (CSRF) est une attaque qui force les utilisateurs authentifiés à soumettre une demande à une application Web par rapport à laquelle ils sont actuellement authentifiés. Les attaques CSRF exploitent la confiance qu'une application Web accorde à un utilisateur authentifié. Cette propriété permet l'utilisation d'un jeton de sécurité pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite. Si `glide.security.use_csrf_token` la valeur recommandée n'est pas définie sur true, CSRF est possible.
Activer l'assainisseur HTML dans Agent virtuel [Mise à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer l'assainisseur HTML dans Agent virtuel • Ancienne description brève : Activer l'assainisseur HTML • Nouvelle description : cette propriété contrôle si HtmlSanitizerService est activé. Si `com.glide.cs.html.sanitizer.enabled` la valeur n'est pas définie sur vrai, une attaque de script de site à site stocké (XSS) est possible dans le client Web VA. • Ancienne description : Cette propriété contrôle si HTMLSanitezerService est activé. Si `com.glide.cs.html.sanitizer.enabled` la valeur n'est pas définie sur vrai, une attaque de script de site à site stocké (XSS) est possible dans le client Web VA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Refuser l’accès interne aux rôles externes explicites [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouveau nom de la configuration technique : *glide.security.explicit_roles.enable_internal_us* • Ancien nom de la configuration technique : *glide.security.explicit_roles.enable_internal_us* • Nouvelle description : cette propriété empêche d’affecter le rôle de snc_internal à des utilisateurs externes. Quand *glide.security.explicit_roles.enable_internal_us* est défini sur la valeur recommandée true, il applique les paramètres de maint-protected *glide.security.explicit_roles.internal_user_blac property* qui affecte le rôle snc_external à une liste de classes d’utilisateurs non approuvés. Si la valeur est définie sur faux, la *glide.security.explicit_roles.internal_user_blac* propriété est ignorée. Une mauvaise configuration de cette propriété augmente le risque qu’un compte d’utilisateur externe accède à des informations internes. • Ancienne description : cela empêche d’affecter le rôle de snc_internal à des utilisateurs externes. Si *glide.security.explicit_roles.enable_internal_us* la propriété n’est pas définie sur la valeur conseillée vrai et que la *glide.security.explicit_roles.internal_user_blac* propriété n’est pas définie sur une liste de classes d’utilisateurs non approuvées, les rôles spécifiés peuvent se voir affecter le rôle snc_internal au lieu du rôle snc_external. Si la liste est vide, tous les utilisateurs se verront attribuer le rôle snc_internal par défaut. La propriété doit contenir au moins les rôles par défaut csm_consumer_user, customer_contact. Une mauvaise configuration de ces propriétés augmente le risque qu’un compte d’utilisateur externe accède aux informations internes. • Nouvelle correction : assurez-vous que la propriété *glide.security.explicit_roles.enable_internal_us* est définie sur true. • Ancien rattrapage : assurez-vous que la propriété *glide.security.explicit_roles.enable_internal_us*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	est définie sur vrai et que la propriété *glide.security.explicit_roles.internal_user_blac* inclut les éléments dangereux csm_consumer_user, customer_contact. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour la demande WSDL [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : si *glide.basicauth.required.wsdl* la valeur n'est pas définie sur la valeur conseillée, vrai, l'authentification de base pour les demandes WSDL est alors désactivée. WSDL est un protocole utilisé pour décrire les services Web tels que les schémas de table d'instance, et n'est pas un mécanisme de partage des données au sein de tables. Définir cette propriété sur vrai permet la divulgation des schémas de table aux utilisateurs non authentifiés. • Ancienne description : si *glide.basicauth.required.wsdl* la valeur recommandée est vrai, l'authentification de base pour les demandes WSDL est alors désactivée. Cela pourrait entraîner la divulgation d'informations à des utilisateurs non authentifiés. • Nouveau score CVSS : 5,3 • Ancien score CVSS : 4,3
Appliquer la vérification de la liste d'autorisations d'URL [Mis à jour dans le Centre de sécurité 1.3, 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Définir les types MIME téléchargeables restreints [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Définir les types MIME téléchargeables restreints • Ancienne description brève : Restreindre les types MIME téléchargeables • Nouvelle description : si *glide.ui.attachment.download_mime_types* elle contient des éléments dangereux tels que text/html, image/svg, image/svg+xml, application/xml, les fichiers dangereux peuvent être affichés en ligne dans le navigateur, ce qui peut entraîner des attaques de script Cross Sitte (XSS). Cette propriété correspond à la liste des types MIME de pièce jointe séparés par des virgules qui ne seront

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	pas affichés en ligne dans le navigateur. Par exemple, l'inclusion de text/html forcera le téléchargement des fichiers HTML vers le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur. La gestion correcte de cette liste évite les attaques de script de site à site. • Ancienne description : si *glide.ui.attachment.download_mime_types* elle contient des éléments dangereux tels que text/html, image/svg, image/svg+xml, application/xml, les fichiers dangereux peuvent être affichés en ligne dans le navigateur, ce qui peut entraîner des attaques de script Cross Sitte (XSS). Cette propriété correspond à la liste des types MIME de pièce jointe séparés par des virgules qui ne seront pas affichés en ligne dans le navigateur. Par exemple, l'inclusion de text/html forcera le téléchargement des fichiers html vers le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur. La gestion correcte de cette liste évite les attaques de script de site à site.
HTML d'échappement dans les vues de listes [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : cette propriété permet de nettoyer l'affichage en vue liste des champs HTML. Si *glide.ui.escape_html_list_field* la valeur n'est pas définie sur la valeur conseillée vrai, un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur. Cela pourrait potentiellement être exploité par des attaquants pour voler des informations de session et des données sensibles. • Ancienne description : La propriété suivante permet de nettoyer l'affichage en vue liste des champs HTML. Si *glide.ui.escape_html_list_field* la valeur n'est pas définie sur la valeur conseillée vrai, un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur. Cela pourrait

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	potentiellement être exploité par des attaquants pour voler des informations de session et des données sensibles.
Restreindre les domaines de messagerie pour l'inscription des utilisateurs externes [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes • Ancienne description brève : Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes (Applicabilité du module d'extension : inscription de l'utilisateur externe) • Nouvelle description : la *sn_ext_usr_reg.allowed_email_domains* propriété définit les adresses e-mail autorisées à s'auto-enregistrer sur une instance ServiceNow. S'il *sn_ext_usr_reg.allowed_email_domains* n'est pas défini avec une liste de domaines acceptables, les utilisateurs avec n'importe quelle adresse e-mail sont autorisés à enregistrer des comptes sur les instances. Si cette propriété n'est pas définie, les acteurs malveillants peuvent effectuer l'enregistrement à l'aide d'adresses e-mail de domaines indésirables pour obtenir un accès authentifié à l'instance. • Ancienne description : S'il *sn_ext_usr_reg.allowed_email_domains* n'est pas défini avec une liste blanche de domaines acceptables, des acteurs malveillants peuvent effectuer l'enregistrement en utilisant des adresses e-mail de domaines indésirables. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer le Captcha pour l'inscription de l'utilisateur externe [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer le Captcha pour l'inscription de l'utilisateur externe • Ancienne description brève : Activer le Captcha pour l'inscription de l'utilisateur externe (Applicabilité du module d'extension : inscription de l'utilisateur externe) • Script de règle : le script a été mis à jour pour améliorer la précision de la détection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Minimiser la durée d'expiration du lien d'inscription de l'utilisateur externe [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe • Ancienne description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe (Applicabilité du module d'extension : inscription de l'utilisateur externe) • Script de règle : le script a été mis à jour pour améliorer la précision de la détection
Désactiver le téléchargement des fichiers infectés [Mis à jour dans Security Center 1.5 et 2.0]	• Nouvelle description brève : Désactiver le téléchargement des fichiers infectés • Ancienne description brève : Interdire le téléchargement des fichiers infectés • Nouvelle correction : assurez-vous que la propriété `com.glide.snap.infected_download_allowed` est définie sur False. • Ancien rattrapage : assurez-vous que la propriété `com.glide.snap.infected_download_allowed` est définie sur Vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Valider le type MIME de fichier dans AttachmentCreator SOAP Web Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description : si `glide.attachment.enforce_security_validation` la valeur n'est pas définie sur la valeur conseillée Vrai, il n'y aura aucune validation pour les pièces jointes de type MIME et des fichiers dangereux pourraient être téléchargés sur le système en utilisant des extensions de fichier incorrectes. Lorsque cette propriété est définie sur vrai, les fichiers sont chargés avec l'extension de type de fichier correcte. Une bonne pratique de sécurité consiste à valider les chargements de fichiers au moins avec la validation de type MIME. • Ancienne description : si `glide.attachment.enforce_security_validation` n'est pas défini sur la valeur recommandée Vrai, il n'y aura aucune validation pour les pièces jointes de type MIME et des fichiers dangereux pourraient être téléchargés sur le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	système en utilisant des extensions de fichier incorrectes. Lorsque cette propriété est définie sur vrai, les fichiers sont chargés avec l'extension de type de fichier correcte. Une bonne pratique de sécurité consiste à valider les chargements de fichiers au moins avec la validation de type MIME. • Nouvelle correction : assurez-vous que la propriété `glide.attachment.enforce_security_validation` est définie sur true. • Ancien rattrapage : assurez-vous que la propriété `glide.attachment.enforce_security_validation` est définie sur Vrai.
Désactiver le débogage MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Désactiver le débogage MultiSSO • Ancienne description brève : Désactiver le débogage MultiSSO (Applicabilité du module d'extension : Authentification unique de plusieurs fournisseurs)
Définir les adresses IP internes autorisées ServiceNow [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouveau nom de la configuration technique : `glide.ip.authenticate.strict` • Ancien nom de la configuration technique : `glide.ip.authenticate.strict,glide.ip.authentica` • Nouvelle description : si `glide.ip.authenticate.strict` la valeur est définie sur vrai, le personnel et les systèmes internes de ServiceNow ne peuvent établir des connexions entrantes à l'instance qu'à partir des plages IP essentielles. Cela limite la visibilité de ServiceNow sur l'instance pour l'infrastructure interne essentielle et empêche l'accès par un personnel ServiceNow plus large, comme le personnel de support et de vente, via les réseaux de l'entreprise. Lorsqu'elle est définie sur « vrai », la `glide.ip.authenticate.allow` propriété est utilisée pour accorder les connexions entrantes ServiceNow internes. Si la valeur n'est pas définie sur true, une plage d'adresses IP internes ServiceNow plus large, telle que définie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	dans *glide.ip.authenticate.allow* est utilisée pour accorder les connexions entrantes ServiceNow internes. • Ancienne description : si *glide.ip.authenticate.strict* la valeur est définie sur vrai, seules les plages IP spécifiées dans *glide.ip.authenticate.allow.secured* peuvent établir des connexions entrantes à l'instance. Cette propriété contient uniquement une liste des plages d'adresses IP internes ServiceNow essentielles (VPN sécurisé, DC). Si *glide.ip.authenticate.allow.secured* n'est pas défini sur la valeur ou la permutation recommandée de « 10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139.0.0/16, 127.0.0.1 » ou la liste de valeurs plus récente « 10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139.0.0/16, 127.0.0.1, 0:0:0:0:0:0:0:1, ::1 » qui ajoute IPv6 localhost à l'Utah, il peut alors permettre à des sources non fiables en dehors du centre de données SN et du VPN sécurisé d'accéder à des sources sensibles en dehors du centre de données SN et du VPN sécurisé Surveillance des points de terminaison sur les instances. • Nouveau rattrapage : assurez-vous que la propriété *glide.ip.authenticate.allow.secured* contient uniquement des valeurs fiables et que la propriété *glide.ip.authenticate.strict* est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété *glide.ip.authenticate.allow.secured* contient uniquement des valeurs dans « 10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139.0.0/16, 127.0.0.1, 0:0:0:0:0:0:0:1, ::1 » et que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.ip.authenticate.strict` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5]	• Nouvelle description brève : Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 • Ancienne description brève : Désactiver l'expansion des entités • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Appliquer Séparation en domaines sur les champs de type « remontée pas à pas » • Ancienne description brève : Appliquer Séparation en domaines sur les champs de type « remontée pas à pas » (Applicabilité du module d'extension : Séparation en domaines) • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les autorisations pour le modèle CMDB [Mis à jour dans Centre de sécurité 1.3 et 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger l'effacement du presse-papiers lors de l'affichage l'application mobile en arrière-plan [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description : la `glide.sg.clear_pasteboard_when_backgrounded` propriété contrôle si le texte copié à partir de l'application mobile ServiceNow est conservé dans le presse-papiers une fois que l'application est en mode arrière-plan. Si elle n'est pas définie sur la valeur conseillée true, les informations sensibles peuvent être divulguées au presse-papiers Android ou iOS, où elles peuvent être exposées à d'autres applications sur l'appareil. • Ancienne description : la propriété `glide.sg.clear_pasteboard_when_backgrounded` contrôle si le texte copié à partir de l'application mobile ServiceNow est conservé dans le presse-papiers une fois que l'application n'est plus active. Si elle n'est pas définie sur la valeur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	conseillée true, les informations sensibles peuvent être divulguées au presse-papiers Android ou iOS, où elles peuvent être exposées à d'autres applications sur l'appareil.
Activer la récupération de compte [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer la récupération de compte • Ancienne description brève : Activer la récupération de compte (Applicabilité du module d'extension : Authentification unique de plusieurs fournisseurs)
Désactiver les messages d'erreur SQL [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : si `glide.db.loguser` la valeur n'est pas définie sur la valeur conseillée, faux, des messages d'erreur sensibles côté serveur peuvent être affichés aux utilisateurs finaux. Les messages d'erreur peuvent inclure des traces de pile et des informations sur la structure de la base de données qui pourraient fournir à un attaquant les connaissances nécessaires pour effectuer une injection SQL réussie si les conditions préalables sont réunies. Dans le cadre d'une défense en profondeur, ces messages d'erreur ne doivent pas être affichés à l'utilisateur final. • Ancienne description : si `glide.db.loguser` la propriété n'est pas définie sur la valeur conseillée, faux, des messages d'erreur sensibles côté serveur peuvent être affichés aux utilisateurs finaux.
Renforcer les liens relatifs [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : la `glide.cms.catalog_uri_relative` propriété applique les liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si `glide.cms.catalog_uri_relative` la valeur recommandée n'est pas définie sur true, l'URL n'est pas assainie avec la fonction enforceRelativeURL(url). Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans le cadre d'un paramètre ou d'une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire. Cette propriété impacte l'ancien système de gestion du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	contenu (CMS) qui a été remplacé par Portail de services. • Ancienne description : la *glide.cms.catalog_uri_relative* propriété applique les liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si *glide.cms.catalog_uri_relative* la valeur recommandée n'est pas définie sur true, l'URL n'est pas assainie avec la fonction enforceRelativeURL(url). Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans le cadre d'un paramètre ou d'une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire.
Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts [mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts • Ancienne description brève : Minimiser le seuil d'expansion des entités • Nouvelle description : cette propriété contrôle la quantité maximale d'expansion d'entité dans un analyseur XML. Si *glide.xmlutil.max_entity_expansion* elle n'est pas définie sur la valeur conseillée de 3 000 ou moins, le script d'analyse GlideXMLUtil peut être vulnérable aux attaques par déni de service. • Ancienne description : cette propriété contrôle la quantité maximale d'expansion d'entité dans un analyseur XML. S'il *glide.xmlutil.max_entity_expansion* n'est pas défini sur la valeur recommandée de 3 000 ou moins, l'analyseur XML peut être vulnérable aux attaques par déni de service. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle description : GlideRecord a fourni un accès de création/mise à jour entre périmètres à des tables qui n'ont pas été configurées avec ce niveau d'accès. Afin d'éviter que les applications des clients ne soient interrompues lorsque ce comportement d'accès inclus dans le périmètre est corrigé, la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	glide.record.legacy_cross_scope_access_policy_in a été créée. Si la valeur est vrai, l'accès entre périmètres revient au comportement hérité (non sécurisé). Cette propriété désactive la séparation des périmètres, ce qui permet aux applications incluses dans le périmètre d'accéder aux interfaces de script globales. Il est préférable de mettre en place des restrictions de clôture de portée. La définition du champ d'application garantit que les applications ne peuvent accéder aux ressources qu'avec un accès explicite ou dans leur champ d'application, conformément au principe du moindre privilège. La désactivation de cette fonctionnalité peut entraîner des impacts sur la confidentialité, la disponibilité et l'intégrité. • Ancienne description : Le comportement hérité fournissait un accès en création/mise à jour aux tables qui ne le permettait pas. Afin d'éviter que les applications des clients hérités ne soient interrompues lors de la correction de ce comportement d'accès inclus dans le champ d'application, la propriété *glide.record.legacy_cross_scope_access_policy_in* a été créée. Si la valeur est vrai, l'accès entre périmètres revient au comportement hérité (non sécurisé). Cette propriété désactive la séparation des périmètres, ce qui permet aux applications incluses dans le périmètre d'accéder aux interfaces de script globales. Il est préférable de mettre en place des restrictions de clôture de portée. La définition du champ d'application garantit que les applications ne peuvent accéder aux ressources qu'avec un accès explicite ou dans leur champ d'application, conformément au principe du moindre privilège. La désactivation de cette fonctionnalité peut entraîner des impacts sur la confidentialité, la disponibilité et l'intégrité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer la version actualisée du module d'extension Multi SSO • Ancienne description brève : Activer la version actualisée du module d'extension Multi SSO (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Activer SSL dans l'authentification LDAP [Mis à jour dans Centre de sécurité 1.5 et 2.0]	Le script a été mis à jour pour améliorer la précision de détection.
Appliquer la réinitialisation du mot de passe aux demandes d'API [Mis à jour dans Centre de sécurité 1.5]	Le script a été mis à jour pour améliorer la précision de détection.
Ne pas appliquer la politique de mot de passe lors de la connexion [Mis à jour dans Centre de sécurité 1.5 et supprimé dans la version 2.0]	• Nouvelle description : en définissant la propriété `glide.apply.password_policy.on_login` sur Faux, il n'y aura pas d'application de la complexité du mot de passe au moment de la connexion. Définir la propriété sur Vrai renforce la complexité du mot de passe et entraîne des problèmes de conformité à la politique de l'organisation. Selon les recommandations de l'ASVS 4.03 v2.1.9 : Vérifiez qu'il n'existe aucune règle de composition de mot de passe limitant le type de caractères autorisés. Il ne devrait pas y avoir d'exigence de majuscules ou de minuscules ou de chiffres ou de caractères spéciaux. (C6) Au lieu d'appliquer la complexité du mot de passe, l'ASVS recommande d'appliquer une longueur minimale de 12 caractères pour la longueur du mot de passe. Réf : authentification OWASP ASVS v4.0 • Ancienne description : Si vous définissez la propriété `glide.apply.password_policy.on_login` sur Faux, aucune application de complexité de mot de passe n'est exécutée au moment de la connexion. Définir la propriété sur Vrai renforce la complexité du mot de passe et entraîne des problèmes de conformité à la politique de l'organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Selon les recommandations de l'ASVS 4.03 v2.1.9 : Vérifiez qu'il n'existe aucune règle de composition de mot de passe limitant le type de caractères autorisés. Il ne devrait pas y avoir d'exigence de majuscules ou de minuscules ou de chiffres ou de caractères spéciaux. (C6) Au lieu d'appliquer la complexité du mot de passe, l'ASVS recommande d'appliquer une longueur minimale de 12 caractères pour la longueur du mot de passe. Réf : authentification OWASP ASVS v4.0
N'utilisez pas de certificats de démonstration pour les configurations SAML actives [Mis à jour dans Centre de sécurité 1.5]	• Nouvelle description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives • Ancienne description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » • Ancienne description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Bloquer les jetons anti-CSRF expirés [Mis à jour dans Centre de sécurité 1.5]	• Nouvelle description brève : Bloquer les jetons anti-CSRF expirés • Ancienne description brève : Bloquer les jetons CSRF expirés
Exiger un captcha pour l'expérience de visite d'un invité dans l'application Service clientèle [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Exiger un Captcha pour l'expérience de visite d'un invité dans l'application Service clientèle • Ancienne description brève : Exiger un Captcha pour l'expérience de visite d'un invité dans l'application Service clientèle

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	(Applicabilité du module d'extension : Expérience de visite des invités pour Service clientèle)
Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH • Ancienne description brève : Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH (Applicabilité du module d'extension : Application dans le champ d'application de Ressources humaines)
Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Restreindre les mises à jour des tickets RH à partir d'e-mails personnels • Ancienne description brève : Restreindre les mises à jour des tickets RH à partir d'e-mails personnels (Applicabilité du module d'extension : Application Ressources humaines incluse dans le périmètre) • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer le journal d'audit MID [nouveau dans Security Center 1.3 et mis à jour dans 1.5]	• Nouvelle description brève : Activer le journal d'audit MID • Ancienne description brève : Activer le journal d'audit MID (Applicabilité du module d'extension : Serveur MID)
Appliquer l'utilisation d'alias d'informations d'identification [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]	• Nouvelle description brève : Appliquer l'utilisation d'alias d'informations d'identification • Ancienne description brève : Appliquer l'utilisation d'alias d'informations d'identification (Applicabilité du module d'extension : Serveur MID)
Instanciateurs de connexions JMS requis [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle description brève : Instanciateurs de connexions JMS requis • Ancienne description brève : Instanciateurs de connexions JMS requis

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	(Applicabilité du module d'extension : Serveur MID) • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Limiter la taille des pièces jointes dans les flux de formation et de prédiction [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Limiter la taille des pièces jointes dans les flux de formation et de prédiction • Ancienne description brève : Limiter la taille des pièces jointes dans les flux de formation et de prédiction (Applicabilité du module d'extension : Intelligence documentaire de la plateforme)
Assurez-vous que les ACL de table d'archivage sont vérifiées [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Consigner les événements d'audit de session [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description : lorsque la propriété `glide.authenticate.session_access.log_audit_ever` Glide est définie sur vrai, les événements d'audit de session sont créés dans la table sys_session_access_audit. Il est recommandé de consigner des informations sur l'accès à une session pour faciliter les enquêtes sur les acteurs malveillants. Les informations enregistrées comprennent l'utilisateur, l'ID de session (non sensible), l'adresse IP, les rôles et les politiques. • Ancienne description : lorsque la propriété `glide.authenticate.session_access.log_audit_ever` Glide est définie sur vrai, les événements d'audit de session sont créés dans la table sys_session_access_audit. Il est recommandé de consigner des informations générales sur l'accès à la session pour faciliter les enquêtes sur les acteurs malveillants. Les informations enregistrées comprennent l'utilisateur, l'ID de session (non sensible), l'adresse IP, les rôles et les politiques.
Appliquer l'accès ACL inclus dans le champ d'application pour les playbooks de demande d'informations [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Appliquer l'accès ACL inclus dans le champ d'application pour les Information Request Playbooks • Ancienne description brève : Appliquer l'accès ACL inclus dans le champ

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	d'application pour les Information Request Playbooks • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Invalider de manière proactive les sessions inactives [nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]	• Nouvelle description : la propriété `glide.active.session.timeout.invalidate.session` Glide contrôle si une session expirée est invalidée de manière proactive avant que le conteneur Tomcat n'invalide la session. Lorsque cette propriété n'est pas définie sur vrai, il peut y avoir un petit intervalle de temps où une session expirée n'est pas invalidée (60+ secondes, selon la taille de la file d'attente). Si une session est détournée, un attaquant peut être en mesure d'utiliser une session pendant cette courte période. • Ancienne description : la propriété `glide.active.session.timeout.invalidate.session` Glide contrôle si une session de délai d'expiration est invalidée de manière proactive avant le conteneur Tomcat. Lorsque cette propriété n'est pas définie sur vrai, il peut y avoir un petit intervalle de temps où une session expirée n'est pas invalidée (60+ secondes, selon la taille de la file d'attente). Si une session est détournée, un attaquant peut être en mesure d'utiliser une session pendant cette courte période.
Limiter la taille du corps de la réponse HTTP [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Limiter la taille du corps de la réponse HTTP • Ancienne description brève : Vérifier que les réponses HTTP ne déclenchent pas d'exception outofMemory en raison de la taille du corps de la réponse

Paramètres de sécurisation renforcée mis à jour pour la version de base de référence 2.0

Certains paramètres de sécurisation renforcée ont été mis à jour avec la sortie de la version de base de Centre de sécurité référence 2.0.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Minimiser le nombre de sessions interactives simultanées [Mis à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le nombre de sessions interactives simultanées • Ancienne description brève : Glide : authentifier le nombre maximal de sessions interactives simultanées
Renforcer l'approbation de certificat [Mis à jour dans Centre de sécurité 1.3, supprimé dans la version 2.0, ajouté dans la version 7.0]	• Nouvelle description brève : Appliquer l'approbation de certificat • Ancienne description brève : Certificat de confiance
Maximiser la complexité du SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Maximiser la complexité du SMS de réinitialisation du mot de passe • Ancienne description brève : Complexité du SMS de réinitialisation du mot de passe
Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer le module d'extension de haute sécurité • Ancienne description brève : Module d'extension de haute sécurité
Appliquer la sécurité stricte des cookies de session [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Appliquer la sécurité stricte des cookies de session • Ancienne description brève : Cookies de session sécurisés
N'utilisez pas de certificats de démonstration pour les configurations SAML actives [Mis à jour dans Centre de sécurité 1.5]	• Nouvelle description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs) • Ancienne description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives
Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Restreindre les packages Java autorisés [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Restreindre les packages Java autorisés • Ancienne description brève : Liste d'autorisation des packages Java
Exiger le brouillage de l'interface utilisateur de l'application mobile [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger le brouillage de l'interface utilisateur de l'application mobile • Ancienne description brève : Brouillage de l'interface utilisateur de l'application mobile
Désactiver l'accès public aux favoris [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Désactiver l'accès public aux favoris • Ancienne description brève : Accès public aux favoris
Échapper à JavaScript [mis à jour dans Centre de sécurité 1.3]	• Nouvelle description : La propriété `glide.html.escape_script` Glide permet de nettoyer les champs HTML. Si `glide.html.escape_script` cette option n'est pas définie sur la valeur conseillée true, les entrées ne seront pas nettoyées pour les champs HTML (codage de sortie) d'un contexte Java back-end en supprimant le JavaScript intégré. Javascript dans les champs HTML peut entraîner des XSS stockés et reflétés. La possibilité d'avoir un XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué. • Ancienne description : la propriété `glide.html.escape_script` Glide permet de nettoyer les champs HTML. Si `glide.html.escape_script`cette option n'est pas définie sur la valeur conseillée true, les entrées ne seront pas nettoyées pour les champs HTML (codage de sortie) d'un contexte Java back-end en supprimant le JavaScript intégré. Javascript dans les champs HTML peut entraîner des XSS stockés et reflétés. La possibilité d'avoir un XSS peut conduire à une escalade de privilège facilement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué.
Définir des options XFrame pour empêcher l'intégration de sites Web tiers [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description courte : Définir des options XFrame pour empêcher l'intégration de sites Web tiers • Ancienne description brève : Options Xframe • Nouvelle description : si *com.glide.cs.embed.xframe_options* la valeur n'est pas définie sur la valeur recommandée DENY ou SAMEORIGIN, le contenu de l'application Web peut être incorporé dans un site tiers à l'aide d'un URI ALLOW-FROM. Autoriser des sites tiers non approuvés pourrait permettre des attaques telles que le détournement de clic. • Ancienne description : si *com.glide.cs.embed.xframe_options* n'est pas défini sur la valeur recommandée DENY ou SAMEORIGIN, le contenu d'une application Web peut être incorporé dans un site tiers à l'aide d'un URI ALLOW-FROM. Autoriser des sites tiers non approuvés pourrait permettre des attaques telles que le détournement de clic. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
HTML d'échappement dans les vues de listes [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : HTML d'échappement dans les vues de listes • Ancienne description brève : HTML d'échappement
Exiger le brouillage de l'interface utilisateur de l'application mobile classique [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger le brouillage de l'interface utilisateur de l'application mobile classique • Ancienne description brève : Brouillage de l'interface utilisateur de l'application mobile classique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Refuser par défaut en cas d'ACL vides [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Refuser par défaut en cas d'ACL vides • Ancienne description brève : Gestionnaire de sécurité Refus par défaut • Nouvelle description : si *glide.sm.default_mode* n'est pas défini sur la valeur recommandée Refuser, le gestionnaire de sécurité hérité de l'instance autorise l'accès à une ressource lorsqu'aucun ACL n'est défini pour cette ressource ou uniquement des ACL au niveau de la table de caractères génériques. En définissant cette option pour autoriser tout ce qui n'a pas d'ACL explicite défini est susceptible d'être manipulé. • Ancienne description : si *glide.sm.default_mode* n'est pas défini sur la valeur recommandée refuser, il autorise l'accès du gestionnaire de sécurité hérité à une ressource lorsqu'aucune ACL n'est définie pour cette ressource ou uniquement des ACL au niveau de la table de caractères génériques. En définissant cette option pour autoriser tout ce qui n'a pas d'ACL explicite défini est susceptible d'être manipulé.
Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe • Ancienne description brève : Fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe
Exiger une autorisation pour les demandes XSD [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes XSD • Ancienne description brève : Autorisation de la demande XSD • Nouveau rattrapage : assurez-vous que la propriété *glide.basicauth.required.xsd* existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.basicauth.required.xsd` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Script Jelly d'échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Script Jelly d'échappement • Ancienne description brève : Jelly d'échappement
Double vérification des transactions entrantes [Mis à jour dans Centre de sécurité 1.3]	• Nouveau rattrapage : assurez-vous que la propriété `glide.security.strict.updates` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.security.strict.updates` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les types de fichiers téléchargeables dans le contenu statique [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Restreindre les types de fichiers téléchargeables dans le contenu statique • Ancienne description brève : Types de fichiers Restrictions de téléchargement du contenu statique
Exiger une autorisation pour les demandes PDF [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes PDF • Ancienne description brève : Autorisation de demande de PDF • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.pdf` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	`glide.basicauth.required.pdf` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les types MIME chargés [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Restreindre les types MIME chargés • Ancienne description brève : Restriction sur le type MIME de téléchargement • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver le comportement JQuery hérité [Mis à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver le comportement JQuery hérité • Ancienne description brève : Comportement JQuery hérité
Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe • Ancienne description brève : Fenêtre de déverrouillage de demande de réinitialisation du mot de passe
Désactiver le débogage MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Désactiver le débogage MultiSSO (Applicabilité du module d'extension : Authentification unique de plusieurs fournisseurs) • Ancienne description brève : Désactiver le débogage MultiSSO • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Appliquer le comportement de l'instance de production [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Appliquer le comportement de l'instance de production • Ancienne description brève : Comportement de l'instance de production

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Limiter les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et mis à jour dans la version 2.0]	• Nouvelle description brève : Minimiser le nombre maximal de tentatives de demande de réinitialisation du mot de passe • Ancienne description brève : Nombre maximal de tentatives de demande de réinitialisation du mot de passe
Exiger une autorisation pour les demandes CSV [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes CSV • Ancienne description brève : Autorisation des demandes CSV • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.csv` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.csv` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser la durée de la fenêtre de succès de demande de réinitialisation de mot de passe [Mis à jour dans Securty Center 1.3]	• Nouvelle description brève : Minimiser la durée de la fenêtre de succès de demande de réinitialisation du mot de passe • Ancienne description brève : Fenêtre de succès de demande de réinitialisation du mot de passe
Appliquer la sécurité stricte des requêtes SOAP [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Appliquer la sécurité stricte des requêtes SOAP • Ancienne description brève : Sécurité stricte des requêtes SOAP
Exiger une autorisation pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Exiger une autorisation pour les demandes SOAP • Ancienne description brève : Autorisation de demande SOAP • Nouvelle description : la propriété `glide.basicauth.required.soap` Glide contrôle si une authentification est requise pour effectuer une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	demande SOAP à une instance. Si `glide.basicauth.required.soap` la valeur recommandée n'est pas définie sur vrai, l'authentification est désactivée pour les demandes SOAP sur l'instance. Il permet un accès non authentifié aux opérations de niveau administrateur ou de maintenance ; annulant ainsi les contrôles de sécurité au sein de l'instance. • Ancienne description : La propriété `glide.basicauth.required.soap` Glide contrôle si une authentification est requise pour effectuer une demande SOAP à une instance. Si glide.basicauth.required.soap n'est pas défini sur la valeur conseillée true, l'authentification est alors désactivée pour les demandes SOAP sur l'instance. Il permet un accès non authentifié aux opérations de niveau administrateur ou de maintenance ; annulant ainsi tous les contrôles de sécurité au sein de l'instance. • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.soap` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.soap` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable • Ancienne description brève : Validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable
Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » (Applicabilité du module d'extension : Séparation de domaine • Ancienne description brève : Appliquer la séparation en domaines

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Nouvelle description : cette propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de type « remontée pas à pas ». Si *glide.sys.domain.include_domain_condition_on_joi* cette propriété n'est pas définie sur la valeur recommandée vrai sur une instance utilisant Séparation de domaine, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique. • Ancienne description : cette propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de remontée pas à pas. Si *glide.sys.domain.include_domain_condition_on_joi* la valeur recommandée est vrai, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique. • Nouvelle correction : assurez-vous que la propriété *glide.sys.domain.include_domain_condition_on_joi* est définie sur vrai lorsque le module d'extension Séparation en domaines est actif. • Ancien rattrapage : assurez-vous que la propriété *glide.sys.domain.include_domain_condition_on_joi* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les demandes JSONP aux URL approuvées [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Restreindre les demandes JSONP aux URL approuvées • Ancienne description brève : Liste d'inclusion de demandes JSONP • Nouvelle description : cette propriété spécifie des URL fiables pour le service de $http AngularJS afin d'autoriser/de rejeter des demandes JSONP. La propriété est nécessaire, car il s'agit d'un changement qui peut avoir des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	conséquences importantes pour les clients, ils ont donc besoin d'un moyen d'ajouter leurs URL de confiance. Si *angular.jsonp.inclusion_list.enabled* la valeur recommandée n'est pas définie sur « vrai », les demandes JSONP sont autorisées pour n'importe quelle URL • Ancienne description : cette propriété spécifie des URL fiables pour le service de $http angularJS afin d'autoriser/ de refuser des demandes JSONP. La propriété est nécessaire, car il s'agit d'un changement qui peut avoir des conséquences importantes pour les clients, ils ont donc besoin d'un moyen d'ajouter leurs URL de confiance. Si *angular.jsonp.inclusion_list.enabled*) n'est pas défini sur la valeur recommandée vrai , les demandes JSONP sont autorisées pour n'importe quelle url.
Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour • Ancienne description brève : Réinitialiser le mot de passe Nombre maximal de SMS par jour
Maximiser la durée du délai de vérification de la réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description courte : Maximiser la durée du délai de vérification de la réinitialisation du mot de passe • Ancienne description brève : Délai de vérification de la réinitialisation du mot de passe • Nouvelle description : si *password_reset.verification.delay* cette propriété n'est pas définie sur la valeur conseillée de 1 000 ou plus, la connexion est plus soumise à des attaques par force brute. Ce délai en millisecondes limite la capacité d'un acteur malveillant à tenter de deviner les détails d'identification ou de vérification des utilisateurs, au moyen d'outils d'automatisation (« bots »). • Ancienne description : si *password_reset.verification.delay* cette propriété n'est pas définie sur la valeur conseillée de 1 000 ou plus, la connexion est plus soumise à des attaques par force brute. Ce délai de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	quelques millisecondes limite la capacité d'un pirate à tenter de deviner les détails d'identification ou de vérification des utilisateurs, en utilisant des outils d'automatisation (« bots »).
Exiger une autorisation pour l'API REST du courtier en données [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour l'API REST du courtier en données • Ancienne description brève : Courtier en données Autorisation REST API • Nouvelle description : si *glide.basicauth.required.databrokerrestapiproces* n'est pas défini sur la valeur recommandée vrai, l'autorisation de base n'est pas requise pour toutes les demandes API REST du courtier en données. Cela peut entraîner une divulgation d'informations non authentifiées de l'instance. • Ancienne description : à compter de la version Utah, si cette option n'est pas définie sur la valeur conseillée « vrai », l'autorisation *glide.basicauth.required.databrokerrestapiproces* de base n'est pas requise pour toutes les demandes entrantes d'API REST du courtier en données. Cela peut entraîner une divulgation d'informations non authentifiées de l'instance. • Nouveau rattrapage : assurez-vous que la propriété *glide.basicauth.required.databrokerrestapiproces* existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété *glide.basicauth.required.databrokerrestapiproces* est définie sur vrai sur les instances exécutant la version Utah et les versions ultérieures. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour la demande JSONv2 [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour la demande JSONv2 • Ancienne description brève : Autorisation de demande JSONv2

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.jsonv2` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.jsonv2` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver les balises JavaScript dans le HTML intégré [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver les balises JavaScript dans le HTML intégré • Ancienne description brève : Autoriser les balises Javascript dans le HTML intégré • Nouvelle correction : assurez-vous que la propriété `glide.ui.security.codetag.allow_script` existe dans la table sys_properties et qu'elle est définie sur faux. • Ancien rattrapage : assurez-vous que la propriété `glide.ui.security.codetag.allow_script` est définie sur false. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) • Ancienne description brève : Module d'extension de démarrage rapide de la sécurité (règles ACL)
Définir l'utilisateur invité pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Définir l'utilisateur invité pour les demandes SOAP • Ancienne description brève : Utilisateur invité pour les demandes SOAP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]	• Nouvelle description brève : Restreindre les entités externes XML • Ancienne description brève : Liste d'autorisation d'URL de validation d'entité XML
Activer les ACL pour contrôler les détails du profil en direct [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer les ACL pour contrôler les détails du profil en direct • Ancienne description brève : Activer les ACL pour contrôler les détails du profil en direct
Restreindre l'accès aux entrées de journal personnalisées [Mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]	• Nouvelle description brève : Restreindre l'accès aux entrées de journal personnalisées • Ancienne description brève : Sécuriser les entrées de journal personnalisées • Nouvelle description : si `glide.live_feed.custom_journal.acl_check_enable` la valeur n'est pas définie sur la valeur conseillée, vrai, tous les utilisateurs peuvent voir toutes les entrées de journal dans la fonctionnalité d'alimentation de vie. Définir la propriété sur vrai permet de respecter les ACL dans les champs de journal personnalisés, ce qui est une fonctionnalité intéressante. • Ancienne description : si `glide.live_feed.custom_journal.acl_check_enable` la valeur n'est pas définie sur la valeur conseillée, vrai, tous les utilisateurs peuvent voir toutes les entrées de journal. Définir la propriété sur vrai permet de respecter les ACL dans les champs de journal personnalisés, ce qui est une fonctionnalité intéressante.
Définir la durée de vie de l'OTP pour la réinitialisation du mot de passe à 1 heure [Mis à jour dans Centre de sécurité 2.0]	• Nouvelle description : cette propriété `glide.pwd_reset.onetime.token.validity` permet au lien contenu dans l'e-mail de réinitialisation du mot de passe d'expirer après le nombre d'heures spécifié dans cette `glide.pwd_reset.onetime.token.validity property`propriété. La durée de validité du jeton de réinitialisation du mot de passe doit être aussi courte que possible en fonction de l'expérience utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	normale. Avoir une longue durée de validité pour le jeton de réinitialisation du mot de passe peut aider les acteurs malveillants à prendre le contrôle du compte. • Ancienne description : cette propriété `glide.pwd_reset.onetime.token.validity` permet au lien contenu dans l'e-mail de réinitialisation du mot de passe d'expirer après le nombre d'heures spécifié dans cette `glide.pwd_reset.onetime.token.validity` propriété. La durée de validité du jeton de réinitialisation du mot de passe doit être aussi courte que possible en fonction de l'expérience utilisateur normale. Avoir une longue durée de validité pour le jeton de réinitialisation du mot de passe peut aider les pirates à prendre le contrôle du compte.
Restreindre l'accès en lecture des développeurs délégués [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Restreindre l'accès en lecture des développeurs délégués • Ancienne description brève : Liste d'autorisation d'accès en lecture pour les développeurs délégués
Définir les adresses IP internes autorisées ServiceNow [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Définir les adresses IP internes ServiceNow autorisées • Ancienne description brève : Adresses IP Liste d'accès autorisé
Valider le type de contenu SOAP [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Valider le type de contenu SOAP • Ancienne description brève : Vérification du type de contenu SOAP • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour les demandes Excel [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes Excel • Ancienne description brève : Autorisation des demandes Excel

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.excel` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.excel` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour les demandes API [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes API • Ancienne description brève : Autorisation des demandes API • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.api` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.api` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts [mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Minimiser le seuil d'expansion des entités • Ancienne description brève : Définition du seuil d'expansion de l'entité
Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe [supprimé dans Centre de sécurité 1.5]	• Nouvelle description brève : Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe • Ancienne description brève : Processus de notification de réinitialisation et de changement de mot de passe • Nouvelle correction : assurez-vous que le processus de réinitialisation du mot de passe avertit les utilisateurs du changement ou de la réinitialisation du mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Ancien rattrapage : assurez-vous que le processus de réinitialisation du mot de passe avertit les utilisateurs du changement ou de la réinitialisation du mot de passe.
Désactiver le comportement AngularJS hérité [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver le comportement AngularJS hérité • Ancienne description brève : Comportement AngularJS hérité
Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion • Ancienne description brève : Gestion du délai d'expiration de déverrouillage après des échecs de connexion
Activer le marqueur de cookie HTTP uniquement [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description courte : Activer le marqueur de cookie HTTP uniquement • Ancienne description brève : Marqueur de cookie HTTP uniquement • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer les ACL d'application administrateur incluses dans le champ d'application [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer les ACL d'application administrateur incluses dans le champ d'application • Ancienne description brève : Administrer les ACL d'application d'administration incluses dans le périmètre • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer UserCookie version 3.1 [Mis à jour dans Centre de sécurité 2.0]	• Nouvelle description : UserCookie v3 est généré uniquement lorsque la propriété `glide.ui.secure.cookies.use_kmf` est désactivée. UserCookie v3 n'est pas sécurisé en raison du stockage de clé secrète pour HMAC dans le code source et identique pour tous les clients. Cela peut permettre à des acteurs malveillants d'utiliser cette clé secrète

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	unique pour tenter de détourner des sessions utilisateurs. • Ancienne description : UserCookie v3 est généré uniquement lorsque la propriété glide.ui.secure.cookies.use_kmf est désactivée. UserCookie v3 n'est pas sécurisé en raison du stockage de clé secrète pour HMAC dans le code source et identique pour tous les clients. Cela peut aider les pirates à utiliser cette clé secrète pour tenter de détourner les sessions des utilisateurs.
Exiger une autorisation pour les demandes XML [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes XML • Ancienne description brève : Autorisation de demande XML • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.xml` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.xml` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser la durée d'expiration du lien d'inscription de l'utilisateur externe [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe • Ancienne description brève : Expiration du lien d'Inscription de l'utilisateur externe
	• Nouvelle description brève : Convertir les images des e-mails entrants en pièces jointes • Ancienne description brève : Convertir les e-mails entrants en HTML
Minimiser la quantité de destinataires SMTP [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la quantité de destinataires SMTP • Ancienne description brève : Nombre maximal de destinataires SMTP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer la version actualisée du module d'extension Multi SSO (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs) • Ancienne description brève : La version mise à jour du module d'extension Multi SSO est activée • Nouveau score CVSS : 7,1 • Ancien score CVSS : 5
Désactiver l'exécution de requêtes de base de données brutes [Mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]	• Nouvelle description brève : Désactiver l'exécution de la requête de base de données brute • Ancienne description brève : Exigences de contrôle d'accès au niveau de l'opération • Nouvelle description : cette propriété permet à un utilisateur d'effectuer des requêtes SQL brutes sur la base de données qui peuvent donner accès à des tables et à des données en dehors des restrictions GlideRecord. Si `glide.db.allow_unsafe_dbi_execute_sql` n'est pas défini sur la valeur recommandée faux, cela permet `d'appeler dbi.executeStatement()` à partir d'un script Glide. • Ancienne description : cette propriété permet à un utilisateur d'effectuer des requêtes SQL brutes sur la base de données qui peuvent donner accès à des tables et à des données en dehors des restrictions GlideRecord. Si `glide.db.allow_unsafe_dbi_execute_sql` n'est pas défini sur la valeur recommandée faux, cela permet `d'appeler dbi.executeStatement()` à partir d'un script Glide.
Balisage XML d'échappement [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Balisage XML d'échappement • Ancienne description brève : XML d'échappement • Nouveau rattrapage : assurez-vous que la propriété `glide.ui.escape_text` existe dans la table sys_properties et qu'elle est définie sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Ancien rattrapage : assurez-vous que la propriété *glide.ui.escape_text* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour les demandes RSS [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes RSS • Ancienne description brève : Autorisation de demande de RSS • Nouveau rattrapage : assurez-vous que la propriété *glide.basicauth.required.rss* existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété *glide.basicauth.required.rss* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Taille maximale autorisée de la pièce jointe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la taille autorisée des pièces jointes • Ancienne description brève : Taille maximale autorisée de la pièce jointe
Renforcer les liens relatifs [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description : la *glide.cms.catalog_uri_relative* propriété applique les liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si *glide.cms.catalog_uri_relative* la valeur recommandée n'est pas définie sur true, l'URL n'est pas assainie avec la fonction enforceRelativeURL(url). Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans le cadre d'un paramètre ou d'une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire. • Ancienne description : utilisez la propriété pour appliquer des *glide.cms.catalog_uri_relative* liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	glide.cms.catalog_uri_relative la valeur n'est pas définie sur la valeur recommandée vrai, l'URL peut ne pas être assainie avec la fonction enforceRelativeURL(url).
Activer la notification du code SMS pour l'inscription et la vérification [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer la notification du code SMS pour l'inscription et la vérification • Ancienne description brève : Notification de code SMS pour l'inscription et la vérification
Valeur d'en-tête HTTP de contrôle de cache [mise à jour dans Centre de sécurité 1.3 et supprimée dans 1.5]	• Nouvelle description brève : Valeur d'en-tête HTTP de contrôle de cache • Ancienne description brève : Valeur d'en-tête HTTP de contrôle de cache • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Refuser l'accès interne aux rôles externes explicites [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Refuser l'accès interne aux rôles externes explicites • Ancienne description brève : Activer les rôles explicites Liste de refus interne • Nouveau nom de la configuration technique : glide.security.explicit_roles.enable_internal_user_blacklist,g • Ancien nom de la configuration technique : glide.security.explicit_roles.enable_internal_user_blacklist • Nouvelle description : cela empêche d'affecter le rôle de snc_internal à des utilisateurs externes. Si *glide.security.explicit_roles.enable_internal_us* la propriété n'est pas définie sur la valeur conseillée vrai et que la *glide.security.explicit_roles.internal_user_blac* propriété n'est pas définie sur une liste de classes d'utilisateurs non approuvées, les rôles spécifiés peuvent se voir affecter le rôle snc_internal au lieu du rôle snc_external. Si la liste est vide, tous les utilisateurs se verront attribuer le rôle snc_internal par défaut. La propriété doit contenir au moins les rôles par défaut csm_consumer_user,customer_contact. Une mauvaise configuration de ces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	propriétés augmente le risque qu'un compte d'utilisateur externe accède aux informations internes. • Ancienne description : cette propriété empêche d'affecter le rôle de snc_internal à des utilisateurs externes. Si *glide.security.explicit_roles.enable_internal_us* la valeur recommandée est vrai, cette option permet *glide.security.explicit_roles.internal_user_blac property* d'affecter snc_external rôle. Si la valeur est définie sur faux, la propriété est désactivée *glide.security.explicit_roles.internal_user_blac* • Nouveau rattrapage : assurez-vous que la propriété *glide.security.explicit_roles.enable_internal_us* est définie sur vrai et que la propriété *glide.security.explicit_roles.internal_user_blac* inclut les éléments dangereux csm_consumer_user, customer_contact. • Ancien rattrapage : assurez-vous que la propriété *glide.security.explicit_roles.enable_internal_us* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser la durée de vie unique du vérificateur hors bande [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description courte : Minimiser la durée de vie unique du vérificateur hors bande • Ancienne description brève : courte durée de vie unique du vérificateur hors bande
Exiger une autorisation pour les demandes de script [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes de script • Ancienne description brève : Autorisation de demande de script • Nouveau rattrapage : assurez-vous que la propriété *glide.basicauth.required.scriptedprocessor* existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	glide.basicauth.required.scriptedprocessor est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Limiter les sessions interactives simultanées [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Limiter les sessions interactives simultanées • Ancienne description brève : Glide : authentifier la limite de sessions interactives simultanées • Nouvelle description : cette propriété est destinée à être utilisée avec le module d'extension Limite de sessions simultanées (*com.glide.limit.concurrent.sessions*). Lorsque le module d'extension est actif et que la propriété est définie sur false, un utilisateur peut avoir un nombre illimité de sessions interactives simultanées sur une instance. Un plus grand nombre de sessions ouvertes signifie qu'il y a une grande possibilité de détournement de session. • Ancienne description : Ce propriétaire est destiné à être utilisé avec le module d'extension Limite de sessions simultanées (*com.glide.limit.concurrent.sessions*). Lorsque le module d'extension est actif et que la propriété est définie sur false, un utilisateur peut avoir un nombre illimité de sessions interactives simultanées sur une instance. Un plus grand nombre de sessions ouvertes signifie qu'il y a une grande possibilité de détournement de session.
Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Appliquer la validation stricte du jeton CSRF • Ancienne description brève : Validation stricte du CSRF • Nouvelle description : cette propriété active la validation stricte des jetons CSRF, ce qui empêche la réutilisation des jetons CSRF. Si *glide.security.csrf.strict.validation.mode* la valeur recommandée n'est pas définie sur vrai, les jetons CSRF peuvent être

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	réutilisés, ce qui ouvre la porte à des attaques CSRF. • Ancienne description : cette propriété active la validation stricte des jetons CSRF, ce qui empêche la réutilisation des jetons CSRF. Si `glide.security.csrf.strict.validation.mode` la valeur n'est pas définie sur la valeur recommandée vrai , le jeton CSRF peut être réutilisé, ce qui ouvre la porte aux attaques CSRF.
Minimiser la durée du délai d'expiration d'activité de la session [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la durée du délai d'expiration d'activité de la session • Ancienne description brève : Délai d'activité de la session
Activer l'assainisseur HTML [mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer l'assainisseur HTML • Ancienne description brève : Assainisseur HTML
Restreindre l'accès au script en arrière-plan [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description : cette propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si `glide.script_processor.admin` elle n'est pas définie sur la valeur recommandée admin, security_admin ou maint, les utilisateurs ayant un rôle avec moins de privilèges seront en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela conduira à un contournement complet du système d'ACL permettant un accès complet aux tables. • Ancienne description : cette propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si `glide.script_processor.admin` cette option n'est pas définie sur la valeur conseillée Administrateur, tout utilisateur ayant un rôle avec peu de privilèges sera en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela conduira à un contournement complet du système d'ACL permettant un accès complet aux tables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Nouvelle correction : assurez-vous que la propriété `glide.script_processor.admin` est définie sur le rôle d'administrateur, de security_admin ou de maintenance. • Ancien rattrapage : assurez-vous que la propriété `glide.script_processor.admin` est définie sur Admin. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver le code HTML intégré [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver le code HTML intégré • Ancienne description brève : Code HTML intégré
Minimiser la durée du délai absolu d'expiration de la session [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la durée du délai absolu d'expiration de la session • Ancienne description brève : Délai absolu de session
Exiger l'authentification par défaut pour les includes de script appelables par le client [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client • Ancienne description brève : Confidentialité sur includes de script pouvant être appelés par le client
Restreindre l'accès à l'API de script GlideSystemUserSession [Mise à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Restreindre l'accès à l'API scriptable GlideSystemUserSession • Ancienne description brève : Accès à l'API scriptable GlideSystemUserSession

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Appliquer l’assainissement HTML [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Appliquer l’assainissement HTML • Ancienne description brève : Vérifier le HTML non nettoyé • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser la durée du délai absolu d’expiration de la session [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la durée du délai absolu d’expiration de la session • Ancienne description brève : Délai absolu de session
Activer l’authentification multifacteur basée sur les rôles [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer l’authentification multifacteur basée sur les rôles • Ancienne description brève : Authentification multifacteur basée sur les rôles
Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » (Applicabilité du module d’extension : authentification unique de plusieurs fournisseurs) • Ancienne description brève : contrainte SAML « notBefore » ou « notOnOrAfter » • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les domaines de messagerie pour l’inscription des utilisateurs externes [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]	• Nouvelle description brève : Restreindre les domaines d’e-mail pour l’inscription des utilisateurs externes (Applicabilité du module d’extension : inscription de l’utilisateur externe) • Ancienne description brève : Liste d’autorisation de domaines de messagerie d’enregistrement d’utilisateurs externes • Nouvelle correction : assurez-vous que la propriété `sn_ext_usr_reg.allowed_email_domains` n’est pas définie sur une valeur vide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	• Ancien rattrapage : assurez-vous que la propriété *sn_ext_usr_reg.allowed_email_domains* n'est pas définie sur une valeur vide.
Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe • Ancienne description brève : Fenêtre de pause SMS de réinitialisation du mot de passe • Nouvelle correction : assurez-vous que la propriété *password_reset.sms.pause_window* est définie sur 2 ou plus. • Ancien rattrapage : assurez-vous que la propriété *password_reset.sms.pause_window* est définie sur 2. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Désactiver les connexions SSLv2/SSLv3 sortantes [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver les connexions SSLv2/SSLv3 sortantes • Ancienne description brève : Désactivation de SSLv2/SSLv3
Exiger une autorisation pour les demandes de déchargement [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes de déchargement • Ancienne description brève : Autorisation de la demande de déchargement • Nouveau rattrapage : assurez-vous que la propriété *glide.basicauth.required.unl* existe dans le sys_properties_table et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété *glide.basicauth.required.unl* est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Activer la notation et le filtrage d'e-mail indésirable [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer le filtrage et la notation des e-mails indésirables • Ancienne description brève : Filtrage et notation d'e-mails indésirables
Annuler le LDAP Nom unique initial [mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]	• Nouvelle description brève : Annuler le nom unique de l'initiale LDAP • Ancienne description brève : Initiale LDAP Nom unique
Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]	• Nouvelle description brève : Activer le jeton anti-CSRF • Ancienne description brève : Jeton anti-CSRF
Exiger la vérification de l'ACL AJAXGlideRecord [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger la vérification de l'ACL AJAXGlideRecord • Ancienne description brève : Activation de la vérification de l'ACL AJAXGlideRecord
Enregistrer l'emprunt d'identité d'un utilisateur [Mis à jour dans Centre de sécurité 1.3 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection. Le script a été mis à jour pour améliorer la précision de détection.
Désactiver le téléchargement des fichiers infectés [Mis à jour dans Security Center 1.5 et 2.0]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer le Captcha pour l'inscription de l'utilisateur externe [mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer le Captcha pour l'inscription de l'utilisateur externe (Applicabilité du module d'extension : inscription de l'utilisateur externe) • Ancienne description brève : Activer le Captcha pour l'inscription de l'utilisateur externe
Désactiver les messages d'erreur SQL [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Désactiver les messages d'erreur SQL • Ancienne description brève : Désactivation des messages d'erreur SQL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Minimiser la durée d'expiration de la demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Minimiser la durée d'expiration de la demande de réinitialisation du mot de passe • Ancienne description brève : Expiration de la demande de réinitialisation du mot de passe • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Délai de verrouillage du contrôle pour les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Minimiser la durée maximale de la fenêtre de demande de réinitialisation du mot de passe • Ancienne description brève : Fenêtre Nombre maximal de tentatives de demande de réinitialisation du mot de passe
Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Restreindre les types MIME téléchargeables • Ancienne description brève : Liste de refus de type MIME téléchargeable
Formules Excel d'échappement [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Formules Excel d'échappement • Ancienne description brève : Formule Excel d'échappement
Activer le module d'extension de sécurité contextuelle [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer le module d'extension de sécurité contextuelle • Ancienne description brève : Module d'extension de sécurité contextuelle
Activer la récupération de compte [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Activer la récupération de compte (Applicabilité du module d'extension : Authentification unique de plusieurs fournisseurs) • Ancienne description brève : Récupération de compte • Nouvelle description : cette propriété contrôle la fonctionnalité de récupération de compte qui lie la possibilité de contourner l'authentification unique aux administrateurs spécifiquement désignés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	Si `glide.sso.acr.enabled` cette option n'est pas définie sur la valeur conseillée true, les connexions interactives locales (basées sur le nom d'utilisateur ou le mot de passe) restent activées lorsque l'authentification unique est activée sur l'instance. L'élimination des connexions interactives locales réduit le risque d'accès non autorisé à l'instance. • Ancienne description : cette propriété contrôle la fonctionnalité de récupération de compte. Si `glide.sso.acr.enabled` cette option n'est pas définie sur la valeur conseillée true, la récupération du compte par userId ne sera pas possible. • Nouveau score CVSS : 6,5 • Ancien score CVSS : 9,1 • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour les demandes d'importation [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes d'importation • Ancienne description brève : Autorisation des demandes d'importation • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.importprocessor` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.importprocessor` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Activer le module d'extension du contrôle d'accès SNC [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Activer le module d'extension du contrôle d'accès SNC • Ancienne description brève : Module d'extension du contrôle d'accès SNC

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Limite de sessions simultanées dans tous les nœuds [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Limite de sessions simultanées dans tous les nœuds • Ancienne description brève : Glide Authentifier la limite de sessions simultanées dans tous les nœuds
Exiger une autorisation pour les demandes de sortie XML [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes de sortie XML • Ancienne description brève : Autorisation de sortie XML • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.xmloutputprocessor` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.xmloutputprocessor` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Scripts d'échappement dans le bloc-notes [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Scripts d'échappement dans le bloc-notes • Ancienne description brève : Bloc-notes d'échappement • Nouvelle description : Le bloc-notes est un moyen facile de définir sur le serveur des informations accessibles dans le navigateur. Un administrateur peut y faire figurer n'importe quoi, y compris des données arbitraires provenant d'enregistrements arbitraires. Si `glide.ui.escape_scratchpad` cette option n'est pas définie sur la valeur conseillée true, il est possible d'exécuter un script malveillant comme une vulnérabilité de script de site à site. • Ancienne description : Le bloc-notes est un moyen facile de définir des informations sur le serveur accessibles dans le navigateur. Un administrateur peut y faire figurer n'importe quoi, y compris des données arbitraires provenant d'enregistrements arbitraires. Si `glide.ui.escape_scratchpad`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	cette option n'est pas définie sur la valeur conseillée true, il est possible d'exécuter un script malveillant comme une vulnérabilité de script de site à site.
Exiger une autorisation pour la demande WSDL [Mis à jour dans Centre de sécurité 1.3 et 1.5]	• Nouvelle description brève : Exiger une autorisation pour la demande WSDL • Ancienne description brève : Autorisation de demande WSDL • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.wsdl` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.wsdl` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Exiger une autorisation pour les demandes SCHEMA [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes SCHEMA • Ancienne description brève : SCHEMA Autorisation de la demande • Nouveau rattrapage : assurez-vous que la propriété `glide.basicauth.required.schema` existe dans la table sys_properties et qu'elle est définie sur vrai. • Ancien rattrapage : assurez-vous que la propriété `glide.basicauth.required.schema` est définie sur vrai. • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]	• Nouvelle description brève : Restreindre les types MIME téléchargeables • Ancienne description brève : Types MIME téléchargeables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Désactiver l'enregistreur pour les utilisateurs avec faibles privilèges dans le bac à sable de script [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver l'enregistreur pour les utilisateurs avec faibles privilèges dans le bac à sable de script • Ancienne description brève : Enregistreur de sécurité Glide Aucune connexion pour le bac à sable • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Implémenter X-Frame-Options : en-tête de sécurité SAMEORIGIN • Ancienne description brève : X-Frame-Options : SAMEORIGIN • Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Restreindre l'accès à la surveillance des performances [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Restreindre l'accès à la surveillance des performances • Ancienne description brève : ACL de surveillance des performances
Désactiver les messages d'erreur SQL détaillé pour le processeur d'importation [Mis à jour dans Centre de sécurité 1.3]	Script de règle : le script a été mis à jour pour améliorer la précision de la détection.
Minimiser la durée d'expiration de SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description courte : Minimiser la durée d'expiration de SMS de réinitialisation du mot de passe • Ancienne description brève : Réinitialiser le mot de passe Expirate de SMS
Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mis à jour dans Centre de sécurité 1.3]	• Nouvelle description brève : Désactiver la création d'utilisateurs à partir d'e-mails entrants • Ancienne description brève : Restreindre les e-mails par domaine • Nouvelle description : un administrateur peut définir une propriété d'e-mail pour créer automatiquement des utilisateurs à partir d'e-mails entrants. Si cette propriété est définie sur la valeur non sécurisée, l'instance crée automatiquement des utilisateurs à partir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	de l'e-mail entrant. Chaque utilisateur créé aura le même mot de passe par défaut codé en dur, ce qui facilite le contournement de l'authentification par force brute. • Ancienne description : un administrateur peut définir une propriété d'e-mail pour créer automatiquement des utilisateurs à partir d'e-mails entrants. Si cette propriété est définie sur la valeur non sécurisée, l'instance crée automatiquement des utilisateurs à partir de l'e-mail entrant. Chaque utilisateur créé aura le même mot de passe par défaut codé en dur, ce qui facilite le contournement de l'authentification par force brute. • Nouvelle correction : assurez-vous que la propriété `glide.pop3readerjob.create_caller` est définie sur false. • Ancien rattrapage : assurez-vous que la propriété `glide.pop3readerjob.create_caller` est définie sur false

Paramètres de sécurisation renforcée supprimés

Certains paramètres de sécurisation renforcée sont supprimés des bases de référence du centre de sécurité.

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 6.0

Certains paramètres de sécurisation renforcée ont été supprimés avec la publication de la version de base de référence 6.0 du Centre de sécurité.

- Appliquer l'ACL sur les données des événements de cycle de vie RH
- Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité
- Appliquer l'ACL sur les données HR Core
- Empêcher les administrateurs globaux de contourner les restrictions d'accès aux applications incluses dans le périmètre
- Désactiver le comportement AngularJS hérité
- Appliquer les ACL au niveau des champs dans GlideRecordSandbox
- Appliquer la sécurité du champ d'application pour Services digitaux pour le secteur public
- Restreindre les types de fichiers téléchargeables dans le contenu statique
- Appliquer l'accès ACL inclus dans le champ d'application pour les Information Request Playbooks
- Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter »

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Restreindre l'accès en lecture des développeurs délégués
- Appliquer la politique de mot de passe à toutes les méthodes
- Appliquer le champ d'application de sécurité pour les informations d'application de service
- Exiger le brouillage de l'interface utilisateur de l'application mobile classique
- Activer SSL dans Authentication LDAP
- Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction
- Supprimer les informations d'identification de la page d'accueil
- Appliquer l'ACL sur les données de l'Agent virtuel RH
- Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH
- Restreindre les packages Java autorisés
- Appliquer des contrôles stricts de signature de code

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 5.0

Certains paramètres de sécurisation renforcée ont été supprimés avec la publication de la version de base de référence 5.0 du Centre de sécurité.

- Exiger l’authentification sur le processeur HTTP de Gestion des événements
- Restreindre l’accès aux entrées de journal personnalisées
- Ne pas appliquer la politique de mot de passe lors de la connexion
- Désactiver l’exécution de la requête de base de données brute
- Nettoyage HTML du journal
- Activer le jeton anti-CSRF
- Appliquer la confiance de certificat
- Annuler le nom unique initial LDAP
- Définir la longueur minimale du mot de passe

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 4.0

Certains paramètres de sécurisation renforcée ont été supprimés avec la sortie de la version de base de Centre de sécurité référence 4.0.

- Mot de passe initial LDAP
- Rôles hors connexion mobiles
- Restreindre l’accès aux données critiques via des politiques d’accès Zero Trust (Applicabilité du module d’extension : authentification adaptative)
- Tables en lecture seule Liste d’autorisation en écriture
- Opérations de sonde JDBC autorisées (Applicabilité du module d’extension : Serveur MID)
- Définir les domaines autorisés qui créent des utilisateurs à partir d’e-mails entrants
- Définir un mot de passe complexe « par défaut »
- Propriétés accessibles dans la liste d’autorisation GraphQL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Liste d'autorisation des messages d'origine croisée
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction pour les points de terminaison GraphQL (Applicabilité du module d'extension : Intelligence documentaire de la plateforme)
- Modifier la liste d'autorisation des rôles de contenu (Applicabilité du module d'extension : Communautés)
- Vérifiez que les requêtes de base de données ne déclenchent pas d'exception OutofMemory en raison de la taille de la requête
- Liste d'autorisation de rôles pour l'exécution du script
- Liste d'autorisation du type de fichier téléchargeable
- Tables en lecture seule Liste d'autorisation de suppression
- Appliquer l'authentification pour l'ACL sans rôle
- Minimiser le délai d'expiration du jeton unique LDAP
- Autoriser uniquement des adresses IP de confiance pour l'authentification
- Définir l'URL de réinitialisation du mot de passe mobile
- Complexité du mot de passe des comptes de service (Applicabilité du module d'extension : Service Bridge)
- Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe
- Appliquer les restrictions du périmètre de l'application
- Exigences de contrôle d'accès (Applicabilité du module d'extension : Communautés)
- Liste d'autorisation de rôles d'accès de l'historique des enregistrements
- Restreindre l'accès du rôle pour les pièces jointes
- Autoriser uniquement les PDF provenant de la liste prédéfinie d'URL de confiance
- Empêcher l'envoi par e-mail d'un mot de passe à usage unique en cas de panne du serveur LDAP
- Convertir les images des e-mails entrants en pièces jointes
- Examiner la condition de contrôle d'accès au rôle explicite superflue

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 2.0

Certains paramètres de sécurisation renforcée ont été supprimés avec la version de base de Centre de sécurité référence 2.0.

- Activer la signature de code pour les données et les scripts de configuration d'application
- Activer le chiffreur KMF Glide
- Désactiver l'utilisation du chiffreur au niveau de l'instance
- Activer la liste de refus interne des rôles explicites
- Bloquer les insertions directes dans la file d'attente ECC MID pour l'exigence de signature de code
- Consigner tous les champs de demande HTTP sortants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôle d'accès

La catégorie de contrôle d'accès audite le processus de protection des ressources contre tout accès non autorisé en accordant et en refusant des demandes basées sur un modèle d'autorisation. Il s'agit notamment de s'assurer qu'une entité accédant à une ressource détient des informations d'identification valides pour ce faire, de créer et de protéger un ensemble bien défini de rôles ou d'autorisations et de s'assurer que les contrôles des rôles ou des autorisations sont protégés contre la relecture et l'altération.

Les contrôles d'accès déterminent si l'accès à une ressource particulière doit être accordé ou refusé. Il n'autorise l'accès aux ressources qu'aux utilisateurs autorisés à les utiliser.

Durée de validation du jeton anti-CSRF [Nouveau dans Security Center 1.3]

La *`glide.security.csrf_previous.time_limit`* propriété spécifie le délai d'expiration d'un jeton de sécurité en secondes.

Lorsqu'une session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la propriété **Autoriser la réutilisation des jetons expirés est** activée et s'il est compris dans la période décrite dans cette propriété. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite.

En savoir plus

Attribut	Description
Nom de la configuration	*`glide.security.csrf_previous.time_limit`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	86400 secondes ou 1 jour
Valeur par défaut	86400 secondes ou 1 jour
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails du risque de sécurité : le fait de ne pas définir cette propriété sur la valeur recommandée désactive la validation de jeton utilisée pour éviter les attaques de contrefaçon de requête intersite.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine la durée en secondes pendant laquelle un jeton de sécurité reste valide. Le jeton de sécurité expire à l'expiration de la session utilisateur, sauf si la propriété **Autoriser la réutilisation des jetons expirés** est activée et le jeton est compris dans la période spécifiée dans cette propriété. Ce jeton empêche les attaques de contrefaçon de requête de site à site. Elle a une valeur par défaut de 86 400 secondes ou 1 jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]

La `glide.sys.domain.include_domain_condition_on_join` propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de type « remontée pas à pas ».

Cette propriété contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de remontée pas à pas. Si `glide.sys.domain.include_domain_condition_on_join` cette propriété n'est pas définie sur la valeur recommandée vrai sur une instance utilisant Séparation de domaine, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique. L'instance peut avoir un impact fonctionnel modéré si les composants dépendent des requêtes interdomaines non sécurisées. Les instances doivent être testées dans des environnements de sous-production avant l'activation.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sys.domain.include_domain_condition_on_join`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Vrai, lorsque Séparation de domaine est installée, sinon la propriété n'existera pas.
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Objectif	Contrôle si les requêtes de jointure reçoivent ou non des conditions séparées par domaine, afin de s'assurer qu'elles appliquent la fonctionnalité Séparation de domaine pour les champs de type « remontée pas à pas ».
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails **du risque** de sécurité : si `glide.sys.domain.include_domain_condition_on_join` cette propriété n'est pas définie sur la valeur recommandée vrai, des informations sensibles peuvent être divulguées et ne doivent pas être partagées avec un domaine spécifique.
Références	Domain Separation pour les fournisseurs de services

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accès en bloc pour les développeurs délégués

Cette configuration affecte l'accès aux développeurs délégués qui mettent à jour les rôles d'utilisateur via le script. Lorsque la configuration est conforme, le développeur ne peut pas mettre à jour ou insérer des enregistrements dans la table de sys_user_has_role sans avoir également le rôle user_admin.

La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance. Lorsque la propriété contient des rôles, seuls ces rôles peuvent exécuter des modules de script.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.sys.security.delegateddev.block_grant_roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance.
Type	interrupteur à bascule
Valeur par défaut	vrai
Valeur recommandée	vrai
Dépendances de Sécurité	aucun
Cote de risque de sécurité	6.7
Impact fonctionnel	Lorsqu'un utilisateur disposant du rôle delegated_developer tente de modifier un enregistrement dans la table sys_user_has_role, cette propriété active des contrôles de sécurité supplémentaires par rapport à l'opération. Les vérifications de sécurité supplémentaires valident que le rôle de user_admin est accordé à l'utilisateur s'il tente de créer ou de mettre à jour la table sys_user_has_role. S'ils n'ont pas le rôle user_admin , l'accès leur sera refusé. Lorsque la propriété est définie sur faux, ces vérifications supplémentaires ne sont pas validées.
Risque de sécurité	(Modéré) Sans autorisation appropriée, les utilisateurs non autorisés peuvent accéder au contenu/aux données sensibles de l'instance.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Bloquer les jetons anti-CSRF expirés [Mis à jour dans Centre de sécurité 1.5]

Bloquez les jetons CSRF expirés pour éviter les attaques de contrefaçon de requête intersite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

Les contrefaçons de requêtes intersites sont un type d'exploit malveillant par lequel des commandes non autorisées sont exécutées au nom d'un utilisateur authentifié.

Détails de la configuration

Attribut	Description
Vue d'ensemble	Contrôle l'utilisation d'un jeton de sécurité expiré pour identifier et valider les demandes entrantes. Définissez la valeur **sur faux** pour empêcher un jeton ayant précédemment expiré de valider une demande entrante.
Nom de la configuration	`glide.security.csrf_previous.allow`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	**false**
Valeur par défaut	**true**
Catégorie	Contrôle d'accès
Risque de sécurité	**Score de gravité** : 6,5
	Évaluation de gravité par score CVSS : moyenne
	Détails du risque de sécurité : applique un mécanisme anti-CSRF puissant pour protéger les fonctionnalités authentifiées, et une protection anti-automatisation ou anti-CSRF efficace protège les fonctionnalités non authentifiées.
Dépendances et prérequis	Aucun
Références	Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0], contrefaçon de requête intersite .

Vérifier les conditions de l'action de l'interface utilisateur avant son exécution

Utilisez la propriété pour activer la `glide.security.strict.actions` vérification des conditions des actions d'interface utilisateur dans les formulaires et les listes avant leur exécution. Lorsque vous définissez cette propriété sur vrai, cela ajoute une couche supplémentaire de validation sur la table actions d'interface utilisateur avant qu'elles ne soient exécutées.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.strict.actions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour assurer une validation supplémentaire sur la table Actions d'interface utilisateur avant leur exécution.
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	3.3
Impact fonctionnel	Cette correction ajoute uniquement une couche supplémentaire de validation pour vérifier les actions d'interface utilisateur sur la table/page cible de l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait pas y avoir d'impact ici.
Risque de sécurité	(Faible) La demande d'accès est toujours vérifiée lorsque des transactions ont lieu entre deux zones. Cette opération valide toutes les actions de l'interface utilisateur avant que le formulaire ne s'affiche pour l'utilisateur final.
Références	Module d'extension de haute sécurité

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Configurer les rôles administrateur du groupe d'affectation de gestion des événements [nouveau dans Security Center 1.5]

Utilisez la `evt_mgmt.connector_assignment_group_admin_roles` propriété pour définir les rôles autorisés pour l'accès administrateur sur le champ Groupe d'affectation dans les instances de connecteur.

La `evt_mgmt.connector_assignment_group_admin_roles` propriété contient une chaîne séparée par des virgules qui indique les noms de rôle disposant d'un accès administrateur sur le champ Groupe d'affectation dans les instances de connecteur. La modification des rôles par défaut dans cette liste peut permettre à des utilisateurs non autorisés de modifier les intégrations d'événements sur l'instance. Pour empêcher tout accès non autorisé aux rôles, définissez `evt_mgmt.connector_assignment_group_admin_roles` la valeur admin,evt_mgmt_admin,sn_sow_srm.srm_admin. Examinez tous les rôles supplémentaires dans la chaîne de valeur recommandée pour vous assurer que le rôle doit être inclus.

En savoir plus

Attribut	Description
Nom de la configuration	`evt_mgmt.connector_assignment_group_admin_roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	administrateur,evt_mgmt_admin,sn_sow_srm.srm_admin
Valeur par défaut	administrateur,evt_mgmt_admin,sn_sow_srm.srm_admin
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : la modification des rôles par défaut peut permettre à des utilisateurs non autorisés de modifier les intégrations d'événements sur l'instance.
Dépendances et prérequis	Aucun
Références	Creating groups

Configurer la liste d'autorisation de widgets du portail de services [Nouveau dans le centre de sécurité 2.0]

Découvrez comment configurer la propriété glide.service_portal.widget.allow_list en toute sécurité afin que les listes de contrôle d'accès (ACL) des tables n'exposent pas d'informations sensibles.

La *glide.service_portal.widget.allow_list* propriété identifie les widgets qui peuvent accéder à n'importe quelle table au sein de l'instance. Toutefois, les listes de contrôle d'accès (ACL) de ces tables continueront de s'appliquer. Si les ACL sont mal configurées ou absentes, les widgets de cette liste peuvent permettre l'accès à ces tables, exposant potentiellement des informations sensibles. Cette propriété n'est efficace que si le widget utilise SNCACLWidgetUtil et que la *glide.service_portal.widget.enforce_public_check* propriété est activée (définie sur vrai).

En savoir plus

Attribut	Description
Nom de la configuration	*glide.service_portal.widget.allow_list*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	tableau
Valeur recommandée	Vide
Valeur par défaut	Vide : dans certains cas de clients, il peut y avoir des valeurs.
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : si vous ne configurez pas cette propriété sur les valeurs recommandées, les widgets peuvent accéder à n'importe quelle table de l'instance.
Dépendances et prérequis	Pour que le *glide.service_portal.widget.allow_list* paramètre soit applicable, la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	`glide.service_portal.widget.enforce_public_check` propriété doit être définie sur vrai.
Impact fonctionnel	Cette propriété permet aux clients d'accéder à n'importe quelle information de table si le widget est défini sur public et est inclus dans la valeur de la propriété.

Configurer la liste d'autorisation de la table des widgets du portail de services [nouveau dans Security Center 2.0]

Découvrez comment la propriété améliore la sécurité en répertoriant les `glide.service_portal.widget.table_allow_list` tables accessibles aux utilisateurs non authentifiés via les widgets du portail de services, en fonction de vérifications supplémentaires et de paramètres de propriété Glide spécifiques.

La `glide.service_portal.widget.table_allow_list` propriété contient une liste de tables auxquelles les utilisateurs non authentifiés peuvent accéder via les widgets du portail de services, qui utilisent les contrôles de sécurité supplémentaires dans le script SNCACLWidgetUtil. Cette propriété n'est appliquée que si la propriété `glide.service_portal.widget.enforce_public_check` Glide est définie sur vrai. L'inclusion de tables inutiles dans cette propriété peut entraîner la divulgation d'informations sensibles. Néanmoins, les ACL de table continueront d'être évaluées comme elles l'étaient auparavant.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.service_portal.widget.table_allow_list`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur sécurisée, des tables inutiles peuvent être incluses, ce qui peut entraîner la divulgation d'informations sensibles.
Dépendances et prérequis	La `glide.service_portal.widget.enforce_public_check` propriété doit être définie sur true pour que le `glide.service_portal.widget.table_allow_list` paramètre prenne effet.
Impact fonctionnel	La liste de tables contrôle l'accès aux tables à partir desquelles le widget est autorisé à récupérer des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Refuser l'accès interne aux rôles externes explicites [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez les propriétés système pour déterminer si le rôle de snc_internal peut être affecté à des utilisateurs externes.

Utilisez la *glide.security.explicit_roles.enable_internal_user_blacklist* propriété système pour empêcher les utilisateurs externes d'être affectés au *snc_internal* rôle. Lorsque cette propriété est définie sur **true**, elle applique les paramètres de la propriété protégée *glide.security.explicit_roles.internal_user_blacklist* par maint. Cette propriété affecte le *snc_external* rôle à une liste de classes d'utilisateurs non approuvés. Si *glide.security.explicit_roles.enable_internal_user_blacklist* la valeur est définie sur **faux**, la *glide.security.explicit_roles.internal_user_blacklist* propriété est ignorée.

Remarque :
Les instances sans rôles explicites installés ne sont pas affectées. À partir de la version Paris, les nouvelles installations d'Explicit Roles obtiennent la propriété avec la valeur par défaut true.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.security.explicit_roles.enable_internal_user_blackl*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Valeur de secours	Faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 5,4 • Score CVSS : moyen • Une mauvaise configuration de cette propriété augmente le risque qu'un compte d'utilisateur externe accède aux informations internes.
Dépendances et prérequis	Aucun

Refuser l'accès non autorisé aux éléments demandés [Mis à jour dans Centre de sécurité 1.3]

La *glide.sc.req_for.roles.default* propriété définit un comportement par défaut pour l'API `retrieveAddress` .

Cette propriété n'est fonctionnelle que lorsqu'elle *glide.sc.req_for.roles* n'a aucune valeur. Si *glide.sc.req_for.roles* elle a des valeurs, cette propriété n'a aucune signification et les utilisateurs ayant uniquement des rôles définis ont accès à l'API.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sc.req_for.roles.default`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Lorsqu'aucun rôle n'est indiqué dans la propriété, l'include de script Client pouvant être appelé `ScriptServiceCatalogGetLocation` peut être appelé par n'importe quel utilisateur connecté sans privilèges et peut récupérer l'adresse de tous les autres utilisateurs du système. Cette propriété protège cette API contre l'exposition des utilisateurs sans privilèges.
Valeur recommandée	refuser
Valeur par défaut	refuser
Type de configuration	Liste de choix (autoriser | refuser)
Risque de sécurité	(Modéré) Si `glide.sc.req_for.roles.default` n'est pas défini sur la valeur recommandée **Refuser** (Autoriser) et que la valeur est `glide.sc.req_for.roles` vide, tout utilisateur peut demander des éléments pour d'autres utilisateurs, autorisant ainsi un accès non autorisé aux ressources.
Références	Includes de script pouvant être appelés par le client

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Afficher des recommandations pour les pages d'interface utilisateur à risque élevé

Réduisez la probabilité d'erreurs d'autorisation et de divulgation d'informations involontaires en affichant des recommandations pour les pages d'interface utilisateur à haut risque.

Utilisez la propriété système **glide.script.ui_page.customer_scoped.security_msgs_enabled** pour déterminer s'il faut afficher des recommandations de sécurité aux utilisateurs qui configurent des pages de l'interface utilisateur lorsque :

- Une ACL est manquante
- Les API GlideRecord/GlideDBQuery sont utilisées à la place de GlideRecordSecure
- La page est configurée comme publique dans la table « sys_public »

Lorsque la propriété est activée, des recommandations lorsque les conditions précédentes sont remplies, ce qui réduit la probabilité d'erreurs d'autorisation et aide à prévenir la divulgation involontaire d'informations.

Définissez la propriété système **glide.script.ui_page.customer_scoped.security_msgs_enabled** sur **vrai** pour afficher ces recommandations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.script.ui_page.customer_scoped.security_msgs_enabled
Applicabilité du module d'extension	Aucun
Risque de sécurité	Définir cette propriété système sur **faux** augmente la probabilité d'erreurs d'autorisation et de divulgation involontaire d'informations.
Score du système de notation des vulnérabilités courantes (CVSS)	5.3
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	Affiche des recommandations de sécurité aux utilisateurs qui configurent des pages de l'interface utilisateur.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	vrai
Valeur de secours	vrai
Valeur recommandée	vrai

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver les e-mails entrants pour les utilisateurs bloqués

Utilisez la propriété pour contrôler les *glide.pop3.process_locked_out* actions sur e-mail entrant pour les utilisateurs actifs et verrouillés.

Définissez cette propriété sur **faux** pour désactiver les e-mails entrants pour les utilisateurs bloqués.

Remarque :
Tenez compte des implications en matière de sécurité de l'autorisation d'utilisateurs de domaines non approuvés, et des raisons pour lesquelles ils ont été bloqués, avant d'autoriser leurs e-mails à déclencher des actions d'e-mails entrants.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.pop3.process_locked_out*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Cette propriété contrôle les actions sur e-mail entrant pour les utilisateurs bloqués.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Risque de sécurité	(Élevé) Lorsque vous définissez cette propriété sur **vrai**, il peut y avoir une divulgation d'informations car les e-mails entrants sont reçus par des utilisateurs ayant des comptes verrouillés.
Cote de risque de sécurité	7.5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Double vérification des transactions entrantes [Mis à jour dans Centre de sécurité 1.3]

Utilisez cette propriété pour activer la double vérification de la sécurité sur les transactions entrantes lors de la `glide.security.strict.updates` soumission d'un formulaire. Lorsque vous définissez cette propriété sur **true**, elle ajoute une couche supplémentaire de validation de table avant qu'un formulaire ne s'affiche dans le navigateur.

Assurez-vous que la propriété `glide.security.strict.updates` existe dans la table sys_properties et qu'elle est définie sur vrai.

En savoir plus

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.security.strict.updates`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour assurer une couche supplémentaire de vérification des autorisations utilisateur avant de présenter le formulaire dans le navigateur.
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	Cette correction ajoute une couche supplémentaire de validation pour vérifier les autorisations utilisateur sur la table/page cible de l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait pas y avoir d'impact.
Risque de sécurité	(Élevé) Vous devez toujours vérifier la demande d'accès lorsque des transactions ont lieu entre deux zones. Cette opération vérifie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	les autorisations lorsque le formulaire est demandé et avant que le rendu du formulaire ne se produise.
Références	Propriétés des paramètres de sécurité

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer les ACL d'application administrateur incluses dans le champ d'application [Mis à jour dans Centre de sécurité 1.3]

Détermine `glide.security.scoped_administration.honor_global_acl` si une application d'administration d'application peut hériter des règles de liste de contrôle d'accès global (ACL).

Cette propriété est particulièrement utile lorsqu'aucune ACL d'application d'administration incluse dans le périmètre n'est définie pour le périmètre de l'enregistrement.

Définissez `glide.security.scoped_administration.honor_global_acl` la valeur sur vrai pour empêcher un utilisateur avec peu de privilèges avec des autorisations dans l'application d'accéder potentiellement à des enregistrements sensibles.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.scoped_administration.honor_global_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Contrôle la règle d'accès ACL dans l'application administrateur incluse dans le périmètre.
Valeur recommandée	Vrai
Valeur par défaut	Vrai
Type de configuration	Booléen
Risque de sécurité	(Faible) Lorsque la valeur de la propriété est définie sur vrai et qu'aucune ACL d'application d'administration incluse dans le périmètre n'est définie pour le champ d'application de l'enregistrement, les ACL globales sont honorées. Si la valeur est définie sur faux, sans qu'aucune ACL d'application d'administration incluse dans le périmètre ne soit définie pour le champ d'application de l'enregistrement, les vérifications d'ACL seront ignorées.
Cote de risque de sécurité	3.8
Références	Access control rules in application administration apps

Pour en savoir plus sur l'activation d'un module d'extension, consultez Activate a plugin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]

Utilisez la propriété pour appliquer des *sn_fsm.use_query_rules* règles et des filtres aux tables de Gestion des services sur site.

Lorsque la valeur est définie sur vrai, les règles/filtres de sn_query_rule table sont utilisés pour déterminer l'accès en lecture aux tables liées à Gestion des services sur site (commande de travaux et tâche de commande de travaux) à l'utilisateur connecté via les règles métier des requêtes et les ACL en lecture. Si la valeur est définie sur false, les enregistrements ne sont pas filtrés en fonction des règles de requête. Les règles métier des requêtes ajoutent des validations de sécurité supplémentaires. Plus précisément, cette propriété filtre les enregistrements d'agents, de qualificateurs et de répartiteurs en fonction du territoire qui leur est affecté ou de leur appartenance au territoire. Il est préférable de suivre le principe du moindre privilège lors de la lecture des documents. Lorsque cette propriété n'est pas définie sur vrai, il peut y avoir un risque accru d'exposition des données des tables Gestion des services sur site.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_fsm.use_query_rules*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : lorsque cette propriété est définie sur vrai, les règles et les filtres de sn_query_rule sont utilisés pour déterminer l'accès en lecture aux tables de Gestion des services sur site, mettant en œuvre le principe du moindre privilège. Lorsque la valeur est définie sur faux, les enregistrements ne sont pas filtrés en fonction des règles métier des requêtes et peuvent présenter un risque accru d'exposition des données des tables de Gestion des services sur site.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque la valeur est définie sur vrai, les règles/filtres de sn_query_rule table sont utilisés pour déterminer l'accès en lecture aux tables associées à Gestion des services sur site. Par exemple, commande de travaux (WO) et table de commande de travaux (WOT) à l'utilisateur connecté via des règles métier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	des requêtes et des ACL en LECTURE. Si la valeur est définie sur false, les enregistrements ne sont pas filtrés en fonction des règles de requête. L'activation de cette propriété sécurise les données et toutes les données (wm_task et wm_order) ne seront pas visibles par leurs utilisateurs.
Références	Field Service Management reference

Activer les ACL pour contrôler les détails du profil en direct [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si un utilisateur doit être en mesure d'afficher tous les champs de détail, tels que le `glide.live_profile.details` nom de la société et les numéros de téléphone, dans un profil actif.

Selon le cadre de la `glide.live_profile.details` propriété, les événements suivants se produisent :

- Si la valeur est définie sur Afficher, l'accès aux informations de profil actif est accordé, quels que soient les ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur ACL, l'accès aux informations de profil actif est restreint, conformément aux ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur Masquer, l'accès aux informations de profil actif est restreint, quels que soient les ACL créées pour le profil d'utilisateur.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.live_profile.details`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	L'objectif est de permettre uniquement aux utilisateurs autorisés d'accéder aux détails d'un profil actif (tels que le nom de la société, les numéros de téléphone)
Type de données	liste de choix
Valeur recommandée	ACL
Valeur par défaut	ACL
Cote de risque de sécurité	4.3
Impact fonctionnel	Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder aux détails du profil actif de tous les autres utilisateurs.
Risque de sécurité	(Modéré) Les demandes d'API doivent toujours honorer les ACL de table. Une restriction doit être appliquée pour empêcher les utilisateurs non autorisés d'accéder aux détails d'un profil actif.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les ACL pour une requête codée dans le widget de liste simple [nouveau dans Centre de sécurité 2.0]

Découvrez comment définir la *glide.service_portal.enable_acls_for_encoded_query_in_list* propriété sur la valeur sécurisée pour empêcher les utilisateurs de contourner les évaluations de la liste de contrôle d'accès (ACL) sur une condition de requête dans le widget de liste simple.

Lorsque la *glide.service_portal.enable_acls_for_encoded_query_in_list* propriété n'est pas définie sur la valeur sécurisée vrai, un utilisateur peut être en mesure de contourner les évaluations de liste de contrôle d'accès (ACL) sur une condition de requête dans le widget Liste simple. Si la propriété est définie sur faux, elle revient au comportement précédent et applique des vérifications d'ACL pour une requête codée en fonction de la valeur de la case à cocher enforce_acl.

La bonne pratique consiste à évaluer les ACL dans les requêtes pour s'assurer qu'un utilisateur a accès aux champs interrogés, empêchant ainsi toute fuite de données non autorisée.

Assurez-vous que la propriété *glide.service_portal.enable_acls_for_encoded_query_in_list* Glide est définie sur true. Si la propriété n'existe pas dans la table sys_properties, la valeur par défaut est vrai.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.script.fencing.cross_scope_access.shared_table_*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée vrai.
Dépendances et prérequis	Aucun
Impact fonctionnel	Le widget Liste simple peut ne pas afficher de données en fonction du rôle de l'utilisateur et des ACL sous-jacentes. En outre, les utilisateurs peuvent rencontrer des avertissements de sécurité si la requête de liste simple contient des conditions de filtre avec des propriétés qui ne sont pas accessibles à l'utilisateur actuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer la liste des URL autorisées pour la communication cross-origin entre iFrame

Utilisez la propriété pour activer la `glide.ui.concourse.onmessage_enforce_same_origin` communication d'origine croisée entre les iframes.

OpenFrame ne peut traiter que les messages provenant de domaines de confiance spécifiés dans la `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` propriété. Pour en savoir plus, consultez Activer la liste des URL autorisées pour la communication cross-origin entre iFrame.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.concourse.onmessage_enforce_same_origin`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Catégorie	Contrôle d'accès
Objectif	Pour activer la liste d'inclusion des domaines de confiance, afin qu'ils puissent communiquer entre les iframes pour openframe.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	4.2
Impact fonctionnel	Si vous n'incluez pas la liste des domaines prévus, la possibilité d'intégrer d'autres pages dans ServiceNow AI Platform les instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas la validation d'origine appropriée, une page Web ou un script de n'importe quelle origine peut communiquer avec elle. Il peut également lancer toute fonctionnalité exécutée par le gestionnaire d'événements.
Références	Vue d'ensemble d'OpenFrame

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]

Utilisez cette `glide.security.use_csrf_token` propriété pour garantir l'utilisation d'un jeton de sécurité pour identifier et valider les demandes entrantes, qui sont ensuite utilisées pour prévenir ces attaques.

La contrefaçon de requête intersite (CSRF) est une attaque qui force les utilisateurs authentifiés à soumettre une demande à une application Web par rapport à laquelle ils sont actuellement authentifiés. Les attaques CSRF exploitent la confiance qu'une application Web accorde à un utilisateur authentifié. Cette propriété permet l'utilisation d'un jeton de sécurité pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite. Si `glide.security.use_csrf_token` la valeur recommandée n'est pas définie sur true, CSRF est possible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.security.use_csrf_token*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour protéger l'application contre une attaque CSRF potentielle.
Cote de risque de sécurité	8.1
Valeur recommandée	vrai
Valeur par défaut	vrai
Impact fonctionnel	Cette correction active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Chaque demande d'écriture contient un jeton CSRF (c'est-à-dire un ID de validation/CSRF lié à la session utilisateur). Lorsque la session utilisateur expire, le jeton de sécurité expire avec elle.
Risque de sécurité	(Élevé) La contrefaçon de requête intersite constitue un risque de sécurité important qui viole l'intégrité des données d'instance. Un attaquant peut lancer l'attaque CSRF en abusant de la confiance d'un utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une demande mal formée au nom de l'attaquant sur l'instance.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le module d'extension de sécurité contextuelle [Mis à jour dans Centre de sécurité 1.3]

Activez le module d'extension de sécurité contextuelle (*com.glide.role_management*) pour activer la sécurité contextuelle, qui sécurise un enregistrement/des informations à l'aide de fonctionnalités de création, de lecture, d'écriture et de suppression.

Après son installation et son activation, les rôles de dictionnaire (créés par Simple Security Manager) ne sont plus testés. Au lieu de cela, le ServiceNow AI Platform recherche les règles ACL sur les champs et les tables. Il sécurise les données à l'aide de règles ACL au lieu des règles de dictionnaire traditionnelles basées sur les rôles mises en œuvre par un simple gestionnaire de sécurité. Même si vous configurez le formulaire de dictionnaire et ajoutez des rôles à une entrée de dictionnaire, aucun changement de droits ne se produit.

En savoir plus

Attribut	Description
ID de module d'extension	*com.glide.role_management*
Type de configuration	Définition du système > Modules d'extension
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Contrairement au gestionnaire de sécurité simple, le gestionnaire de sécurité contextuelle connaît la hiérarchie de la table système. Vous pouvez potentiellement avoir différentes règles de sécurité pour un champ en fonction de l'emplacement dans la hiérarchie où il apparaît.
Valeur recommandée	Actif
Valeur par défaut	Il n'y a pas de valeur par défaut, car il s'agit d'un module d'extension et non d'une propriété Glide.
Cote de risque de sécurité	8.1
Impact fonctionnel	Cette correction applique le niveau fonctionnel des contrôles d'accès, ce qui permettrait à l'application de déterminer les restrictions d'accès en se basant uniquement sur la table d'ACL.
Risque de sécurité	(Élevé) Les contrôles d'accès au niveau fonctionnel doivent être appliqués du côté serveur avant d'exécuter des opérations CRUD, afin de garantir le niveau d'accès approprié pour les utilisateurs de l'instance.
Références	Gestionnaire de sécurité contextuelle

Activer les vérifications de privilège entre périmètres sur le formulaire du portail de services [Nouveautés dans Security Center 7.0]

Utilisez une propriété système pour appliquer les contrôles de privilège entre périmètres sur le widget de formulaire du portail de services et empêcher la récupération non autorisée des données de formulaires et de tables entre les périmètres.

Dans Yokohama les versions et versions ultérieures, les requêtes appliquent des vérifications de privilège entre périmètres sur la table avant de lire les informations sys_id données.

Lorsque la `glide.service_portal.enforce_cross_scope_check_in_form` propriété est définie sur la valeur conseillée **vrai,** les contrôles de privilège entre périmètres sont appliqués à la table. Lorsque la valeur est définie sur **faux**, la vérification de privilège entre périmètres n'est pas appliquée.

Définissez la `glide.service_portal.enforce_cross_scope_check_in_form` propriété système sur **vrai** ou confirmez que la propriété n'existe pas dans la table Propriétés système [sys_properties]. Si aucun enregistrement n'existe dans la table sys_properties, la valeur par défaut est **true**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.service_portal.enforce_cross_scope_check_in_form`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : l'absence de contrôles de privilège entre périmètres peut entraîner une récupération non autorisée des données de formulaires et de tables entre les périmètres.
Dépendances et prérequis	Aucun

Appliquer l'ACL sur les données des événements de cycle de vie RH [nouveau dans Security Center 2.0]

Découvrez comment empêcher tout accès non autorisé aux données de l'application Human Resources Lifecycle Events en vérifiant que la `glide.enforce_security_scope.sn_hr_le property` valeur est définie sur Sécurisé.

La `glide.enforce_security_scope.sn_hr_le` propriété limite les listes de contrôle d'accès (ACL) de plusieurs tables RH afin que seul le périmètre « sn_hr_le » soit pris en compte. Si `glide.enforce_security_scope.sn_hr_le` la valeur recommandée est true, les données de l'application Human Resources : Lifecycle Events seront exposées aux ACL de tous les autres champs d'application, ce qui pourrait entraîner l'accès d'utilisateurs non autorisés à des données sensibles. Par exemple, un administrateur informatique qui accède aux données RH.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_hr_le`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : le fait de ne pas définir cette propriété sur la valeur vrai peut entraîner l'exposition des données de l'application Ressources humaines : événements de cycle de vie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	aux ACL de tous les autres périmètres. Cela peut conduire des utilisateurs non autorisés à accéder à des données sensibles.
Dépendances et prérequis	Aucun

Appliquer l'ACL sur les données HR Core [nouveau dans Security Center 2.0]

Découvrez comment configurer la `glide.enforce_security_scope.sn_hr_core` propriété de sorte que le module d'extension Human Resources Scoped App : Core (com.sn_hr_core) n'expose pas de données sensibles aux listes de contrôle d'accès (ACL) de tous les autres champs d'application.

La `glide.enforce_security_scope.sn_hr_core` propriété restreint les listes de contrôle d'accès (ACL) de plusieurs tables de données globales telles que sys_attachment et sys_email afin de ne prendre en compte que le périmètre sn_hr_core. Si cette propriété n'est pas définie sur la valeur conseillée vrai, les données du module d'extension Application dans le périmètre de ressources humaines : Core seront exposées aux ACL de tous les autres champs d'application. Par exemple, cela peut entraîner l'accès de l'administrateur informatique aux données relatives aux ressources humaines.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_hr_core`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur sécurisée true, les données du module d'extension Application Ressources humaines incluse dans le périmètre : Core seront exposées aux ACL de tous les autres périmètres.
Dépendances et prérequis	Aucun
Références	Activate Case and Knowledge Management

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer l'ACL sur les données de l'Agent virtuel RH [nouveau dans Security Center 2.0]

Découvrez comment définir la *glide.enforce_security_scope.sn_hr_va* propriété sur une valeur sécurisée, empêchant ainsi les fuites de données à partir de l'application incluse dans le périmètre Conversations d'agent virtuel.

La *glide.enforce_security_scope.sn_hr_va* propriété restreint les listes de contrôle d'accès (ACL) de plusieurs tables Human Resources (HR) pour ne prendre en compte que le périmètre sn_hr_va. Si cette propriété n'est pas définie sur la valeur conseillée vrai, les données de l'application incluse dans le périmètre Ressources humaines : conversations de l'agent virtuel seront exposées aux ACL de tous les autres champs d'application. Par exemple, cela pourrait permettre à l'administrateur informatique d'accéder aux données RH.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.enforce_security_scope.sn_hr_va*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur la valeur sécurisée vrai, des données de l'application incluse dans le périmètre Ressources humaines : conversations d'agent virtuel peuvent être exposées aux ACL de tous les autres champs d'application.
Dépendances et prérequis	Aucun

Traduction automatique

Appliquer des ACL spécifiques à l'application uniquement pour les données d'application

Évitez tout accès non autorisé ou indésirable aux données d'application en appliquant des listes de contrôle d'accès (ACL) spécifiques à l'application uniquement pour les données d'application.

Contrôlez le comportement des données d'application résidant dans des tables primaires en dehors de l'application. Lorsque la valeur **de ces** propriétés est true, seules les ACL spécifiques à l'application sont évaluées pour déterminer l'accès aux données d'application résidant dans ces tables. Toutes les applications ne sont pas conçues pour fonctionner dans cette configuration ou n'utilisent pas d'enregistrement de propriété système [sys_properties] à cette fin.

Ces propriétés système utilisent le format de dénomination **glide.enforce_security_scope.<scope>** . Par exemple, utilisez la propriété

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

glide.enforce_security_scope.sn_hr_sp pour le périmètre Centre des employés Core (sn_hr_sp). Les périmètres d'application suivants contiennent cette propriété :

- sn_doc
- sn_egd_act
- sn_egd_core
- sn_egd_goals
- sn_em
- sn_gsm
- sn_gsm_info_req
- sn_gsm_lic_prmt
- sn_gsm_lic_prmt_ex
- sn_gsm_soc_bnfts
- sn_hc_professional
- sn_hr_agent_ws
- sn_hr_ai_agents
- sn_hr_awa
- sn_hr_core
- sn_hr_ef
- sn_hr_er
- sn_hr_gen_ai
- sn_hr_hc
- sn_hr_le
- sn_hr_le_ent
- sn_hr_mii_base
- sn_hr_na_galileo
- sn_hr_pad
- sn_hr_pj
- sn_hr_sp
- sn_hr_va
- sn_hr_ws
- sn_imt_health_test
- sn_imt_tracing
- sn_imt_vaccine
- sn_ja
- sn_jny
- sn_lg_contracts
- sn_lg_matter
- sn_lg_ops
- sn_opp_market
- sn_professional
- sn_svc_appl_info
- sn_svc_appl_pgm_mg
- sn_talent_aia
- sn_uni_req
- sn_uni_task

Pour chaque application installée avec la *glide.enforce_security_scope* propriété dans la table Propriétés système [sys_properties], (par exemple, *glide.enforce_security_scope.sn_hr_core*), assurez-vous que la valeur de la propriété est définie sur **vrai**.

Remarque :
Ces propriétés ne peuvent être modifiées que par l'administrateur du champ d'application pour l'application spécifique. Si un enregistrement sys_properties n'existe pas pour l'application donnée et la propriété respective, il doit être créé.

Utilisez cette fonction de script pour identifier les propriétés qui doivent être mises à jour ou créées sur l'instance :

```
var properties = [
    'glide.enforce_security_scope.sn_uni_task',
    'glide.enforce_security_scope.sn_uni_req',
    'glide.enforce_security_scope.sn_svc_appl_info',
    'glide.enforce_security_scope.sn_professional',
    'glide.enforce_security_scope.sn_opp_market',
    'glide.enforce_security_scope.sn_lg_ops',
    'glide.enforce_security_scope.sn_lg_matter',
    'glide.enforce_security_scope.sn_lg_contracts',
    'glide.enforce_security_scope.sn_jny',
    'glide.enforce_security_scope.sn_ja',
    'glide.enforce_security_scope.sn_imt_vaccine',
    'glide.enforce_security_scope.sn_imt_tracing',
    'glide.enforce_security_scope.sn_imt_health_test',
    'glide.enforce_security_scope.sn_hr_ws',
    'glide.enforce_security_scope.sn_hr_va',
    'glide.enforce_security_scope.sn_hr_sp',
    'glide.enforce_security_scope.sn_hr_pj',
    'glide.enforce_security_scope.sn_hr_pad',
    'glide.enforce_security_scope.sn_hr_mii_base',
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    'glide.enforce_security_scope.sn_hr_le',
    'glide.enforce_security_scope.sn_hr_le_ent',
    'glide.enforce_security_scope.sn_hr_hc',
    'glide.enforce_security_scope.sn_hr_gen_ai',
    'glide.enforce_security_scope.sn_hr_er',
    'glide.enforce_security_scope.sn_hr_ef',
    'glide.enforce_security_scope.sn_hr_core',
    'glide.enforce_security_scope.sn_hr_awa',
    'glide.enforce_security_scope.sn_hr_agent_ws',
    'glide.enforce_security_scope.sn_hc_professional',
    'glide.enforce_security_scope.sn_gsm_soc_bnfts',
    'glide.enforce_security_scope.sn_gsm_lic_prmt_ex',
    'glide.enforce_security_scope.sn_gsm_lic_prmt',
    'glide.enforce_security_scope.sn_gsm_info_req',
    'glide.enforce_security_scope.sn_gsm',
    'glide.enforce_security_scope.sn_em',
    'glide.enforce_security_scope.sn_egd_goals',
    'glide.enforce_security_scope.sn_egd_core',
    'glide.enforce_security_scope.sn_egd_act',
    'glide.enforce_security_scope.sn_doc',
    'glide.enforce_security_scope.sn_talent_aia',
    'glide.enforce_security_scope.sn_hr_na_galileo',
    'glide.enforce_security_scope.sn_svc_appl_pgm_mg',
    'glide.enforce_security_scope.sn_hr_ai_agents',
    'glide.enforce_security_scope.sn_hr_mii_base'
];

var pm = new GlidePluginManager();

for (var i = 0; i < properties.length; i++) {
    var property = properties[i];
    var application = property.split('.')[2];
    var propertyValue = gs.getProperty(property, 'false');

    if (pm.isActive(application) && propertyValue.toLowerCase() != 'true') {
        gs.print(property);
    }
}
```

En savoir plus

Attribut	Description
Nom de la configuration	*glide.enforce_security_scope.<scope>*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,1 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : lorsque ces propriétés n'ont pas la valeur **vrai**, l'accès aux ACL de la table primaire est toujours évalué, ce qui peut permettre un accès non autorisé ou indésirable aux données de l'application.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Appliquer les restrictions du périmètre de l'application [nouveau dans Security Center 1.3 et supprimé dans la version 1.5]

Utilisez la propriété pour contrôler les autorisations des applications incluses dans le `glide.record.legacy_cross_scope_access_policy_in_script` périmètre.

Si la propriété est définie sur vrai, les applications incluses dans le `glide.record.legacy_cross_scope_access_policy_in_script` périmètre peuvent appeler des API qui ne doivent être disponibles que pour les applications globales. Cette propriété contourne les contrôles d'accès prévus pour la création et la mise à jour des développeurs pour ces applications incluses dans le périmètre.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.record.legacy_cross_scope_access_policy_in_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	faux
Valeur par défaut	vrai (lorsque la propriété n'existe pas dans la table sys_properties.)
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée, les applications incluses dans le périmètre et les développeurs délégués pour ces applications incluses dans le périmètre peuvent créer et mettre à jour des enregistrements dans des tables globales telles que Incident.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les rôles de lecture pour la recherche de variables de catalogue [Nouveautés de Security Center 7.0]

Utilisez les propriétés système pour vous assurer que seules les variables de catalogue avec un rôle de lecture vide sont indexées pour la recherche.

Lorsque la propriété *glide.ais.ingestion.ignore_catalog_variables_read_roles* est définie sur la valeur recommandée **faux**, seules les variables de catalogue avec un rôle de lecture vide sont indexées pour la recherche. Si cette propriété est définie sur **vrai** , toutes les variables sont indexées pour la recherche, quels que soient les rôles de lecture spécifiés sur la variable.

Vérifiez que la propriété système n'existe *glide.ais.ingestion.ignore_catalog_variables_read_roles* pas dans la table Propriétés système [sys_properties], ou qu'elle existe et qu'elle est définie sur **false**.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.ais.ingestion.ignore_catalog_variables_read_roles*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Impact fonctionnel	Cette propriété affecte l'indexation du contenu pouvant être recherché à partir de variables de catalogue qui nécessitent des rôles spécifiques pour l'accès en lecture.
Risque de sécurité	• Score de gravité : 2,6 • Score CVSS : faible • Détails du risque de sécurité : les utilisateurs pourront rechercher des variables auxquelles ils n'ont pas accès avec des rôles de lecture entraînant la divulgation d'informations.
Dépendances	Aucun
Références	Service catalog variables

Appliquer des règles de sécurité au partage de tableaux de bord [nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler si les *glide.cms.dashboards.sharing_with_secure_search* utilisateurs peuvent partager des tableaux de bord.

Lorsque la propriété n'est pas définie sur **vrai**, les *glide.cms.dashboards.sharing_with_secure_search* utilisateurs peuvent partager des groupes de tableaux de bord et des rôles auxquels ils n'ont pas accès. L'activation de cette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

propriété applique les listes de contrôle d'accès (ACL) lors de la recherche dans les tables sys_user, sys_user_role et sys_user_group pendant le processus de partage de tableau de bord. Un partage excessif d'un tableau de bord peut amener des utilisateurs, des groupes ou des rôles à accéder à des données qu'ils ne devraient pas être autorisés à consulter, ce qui peut compromettre des informations sensibles. Par conséquent, il est recommandé de définir la valeur *glide.cms.dashboards.sharing_with_secure_search* sur vrai afin que les tableaux de bord ne soient partagés qu'avec ceux qui disposent des autorisations appropriées.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.cms.dashboards.sharing_with_secure_search*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : le fait de ne pas définir cette propriété sur la valeur recommandée vrai entraîne le non-respect des listes de contrôle d'accès lors de la recherche des tables sys_user, sys_user_role et sys_user_group. Cela peut conduire à ce que les tableaux de bord soient partagés avec des utilisateurs non autorisés, exposant ainsi des informations sensibles.
Dépendances et prérequis	Aucun
Références	Access control
Impact fonctionnel	Cette propriété applique des règles de sécurité à la liste d'utilisateurs, de groupes d'utilisateurs et de rôles qui sont visibles lors du partage de tableaux de bord.

Traduction automatique

Appliquer la sécurité du champ d'application pour les services digitaux du secteur public [nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler la *glide.enforce_security_scope.sn_gsm* manière dont vous pouvez accéder aux données de l'application Public Sector Digital Services.

Cette ServiceNow Services digitaux pour le secteur public application vous permet de développer des applications du secteur public qui fournissent des services numériques aux citoyens, aux entreprises et aux agences.

Lorsque *glide.enforce_security_scope.sn_gsm* cette option est définie sur faux, l'accès aux données d'application dans les tables globales de l'application Services digitaux pour le secteur public peut être accessible en fonction des listes de contrôle d'accès (ACL)

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de ces tables globales. Lorsque cette propriété est définie sur vrai, l'accès aux données résidant dans les tables globales est uniquement évalué en fonction des ACL expédiées directement dans l'application Public Sector Digital Services. Définir cette propriété sur faux peut entraîner la divulgation d'informations à partir d'ACL trop permissives.

Pour remédier à ce risque de sécurité, définissez sur *glide.enforce_security_scope.sn_gsm* vrai.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.enforce_security_scope.sn_gsm*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée peut entraîner la divulgation d'informations par des ACL trop permissives.
Dépendances et prérequis	Aucun
Références	Configuring Public Sector Digital Services

Appliquer l'accès ACL inclus dans le champ d'application pour les playbooks de demande d'informations [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Utilisez la propriété pour contrôler l'accès *glide.enforce_security_scope.sn_gsm_info_req* aux données du playbook pour la fonctionnalité Information Request Playbooks.

L'application Information Request Playbook permet aux utilisateurs finaux du secteur public de soumettre et de suivre des demandes d'enregistrements publics et fournit aux agents gouvernementaux un processus prédéfini pour le traitement et la résolution de ces demandes. Si *glide.enforce_security_scope.sn_gsm_info_req* la valeur n'est pas définie sur vrai, un accès inattendu peut être accordé aux données du playbook pour l'application Information Request Playbooks. Définissez cette propriété sur vrai pour ne prendre en compte que les ACL du périmètre sn_gsm_info_req lors de l'octroi de l'accès.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.enforce_security_scope.sn_gsm_info_req*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété est définie sur faux, les ACL de tous les périmètres sont prises en compte lors de l'octroi de l'accès aux données du playbook dans la table maître du périmètre. Cela exposerait les données du playbook de demande d'informations.
Dépendances et prérequis	Aucun
Références	• Using Information Request Playbook • Configure Information Requests service channel

Appliquer le privilège d'élévation stricte [nouveau dans Security Center 1.3]

Utilisez la `glide.security.strict_elevate_privilege` propriété pour contrôler si les rôles marqués comme privilégiés doivent être élevés manuellement pour que les options du rôle soient attribuées à l'utilisateur.

Définissez cette propriété sur vrai pour ajouter une couche supplémentaire de validation de sécurité lorsqu'un utilisateur privilégié élève son rôle.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.strict_elevate_privilege`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : lorsque `glide.security.strict_elevate_privilege` cette option est définie sur faux, les rôles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	marqués comme privilégiés sont automatiquement élevés lors de la nouvelle session d'un utilisateur administrateur et n'ont pas besoin d'être élevés manuellement (à l'exception de security_admin).
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété exige strictement que les utilisateurs avec le rôle administrateur élèvent leurs privilèges lorsque cela est nécessaire.

Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]

Utilisez cette propriété pour déterminer si seules les listes de contrôle d'accès (ACL) du module d'extension Licence et autorisation sont utilisées pour déterminer l'accès au champ d'application, ou si les ACL de tous les champs d'application sont prises en compte.

Lorsque la `glide.enforce_security_scope.sn_gsm_lic_prmt` propriété est définie sur la valeur conseillée true, seules les ACL du module d'extension Licence et autorisation sont utilisées pour déterminer l'accès au champ d'application. Lorsque ce paramètre est configuré sur faux, les données de Licence et autorisation des playbooks dans les tables principales du périmètre sont exposées, car l'accès est accordé aux ACL de tous les périmètres. Pour réduire l'exposition des données, définissez `glide.enforce_security_scope.sn_gsm_lic_prmt` la valeur recommandée sur vrai.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_gsm_lic_prmt`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : la configuration de ce paramètre sur la valeur recommandée vrai sécurise les données de Licence et d'autorisation dans les tables principales du périmètre en tenant compte uniquement des ACL du `sn_gsm_lic_prmt` périmètre pour accorder l'accès. Si vous définissez ceci sur faux, les données de Licence et autorisation des playbooks s'exposent dans les tables principales du périmètre en tenant compte des ACL de tous les périmètres pour accorder l'accès. Par exemple, l'administrateur IT peut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	accéder aux données des Playbooks de licences et d'autorisations lorsque ce paramètre est défini sur faux.
Dépendances et prérequis	Aucun
Références	• Using License and Permit Playbook • Application scope

Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH [Nouveau dans Security Center 1.5 et mis à jour dans la version 2.0]

Configurez le module d'extension Espace de travail d'agent pour la gestion des tickets RH de sorte que seuls les utilisateurs ayant les autorisations appropriées puissent accéder aux données figurant dans les tables principales du champ d'application, en application du principe du moindre privilège.

Lorsque le `glide.enforce_security_scope.sn_hr_agent_ws` module d'extension est configuré sur la valeur recommandée true, seules les listes de contrôle d'accès (ACL) du module d'extension Espace de travail d'agent pour la gestion des tickets RH sont utilisées pour déterminer l'accès à une ressource. Lorsque ce paramètre est défini sur faux, les données d'Espace de travail d'agent pour la gestion des tickets RH dans les tables principales du périmètre sont exposées, car l'accès est accordé aux ACL de tous les périmètres.Par exemple, un administrateur informatique peut accéder aux données d'Espace de travail d'agent pour la gestion des tickets RH lorsque ce paramètre est défini sur faux. Pour éviter que cela ne se produise, définissez `glide.enforce_security_scope.sn_hr_agent_ws` la valeur recommandée sur vrai pour garantir que le principe du moindre privilège existe, car les utilisateurs ne peuvent accéder qu'aux ressources auxquelles ils ont l'autorisation.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_hr_agent_ws`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : si vous configurez ce paramètre sur faux, les données d'Espace de travail d'agent pour la gestion des tickets RH

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	dans les tables principales du périmètre sont exposées, car l'accès est accordé aux ACL de tous les périmètres.
Dépendances et prérequis	Agent Workspace for HR Case Management
Impact fonctionnel	La configuration de ce paramètre sur vrai impose l'exécution des ACL globales pour une table, si les ACL incluses dans le périmètre n'existent pas pour celle-ci.
Références	• https://owasp.org/www-project-proactive-controls/#div-numbering • Add a component to Agent Workspace

Appliquer le champ d'application de sécurité pour les informations d'application de service [nouveau dans Security Center 2.0]

Utilisez la `glide.enforce_security_scope.sn_svc_appl` propriété pour vous assurer que les données des tables du périmètre principal sont sécurisées.

Lorsque la `glide.enforce_security_scope.sn_svc_appl_info` propriété est définie sur vrai, l'accès aux ressources dans le champ d'application est déterminé uniquement par les listes de contrôle d'accès (ACL) du module d'extension Informations sur l'application de service (sn_svc_appl_info). Cela garantit la sécurité des données dans les tables du périmètre principal en limitant les autorisations d'accès à celles définies dans le périmètre sn_svc_appl_info.

Si la valeur non sécurisée est false, les ACL de tous les champs d'application sont prises en compte lors de l'octroi de l'accès aux données dans les tables du champ d'application principal telles que sys_attachment. Cela peut entraîner un accès non autorisé à des informations sensibles par des utilisateurs qui ne disposent pas d'autorisations pour les données d'informations d'application de service.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_svc_appl_info`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété est définie sur la valeur non sécurisée faux, cela peut entraîner un accès non autorisé à des données

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	sensibles par des utilisateurs qui ne disposent pas des autorisations pour les données d'informations sur l'application de service.
Dépendances et prérequis	Le module d'extension Informations du demandeur de service (`com.sn_svc_appl_info`) doit être activé pour que la `glide.enforce_security_scope.sn_svc_appl_info` propriété soit efficace.

Appliquer les ACL au niveau des champs dans GlideRecordSandbox

Gérez les ACL au niveau des champs dans GlideRecordSandbox sur votre instance.

Utilisez cette`glide.sandbox.fields.check_acl` propriété pour appliquer les ACL au niveau des champs dans GlideRecordSandbox. Par exemple, cette propriété est appliquée lorsqu'un utilisateur peut fournir un script, comme dans `sysparm_query`. Si cette propriété n'est pas définie sur la valeur recommandée **vrai**, les restrictions ACL peuvent être contournées, ce qui permet de compromettre les données sensibles, par exemple celles `sys_user.user_password` d'un utilisateur non autorisé.

⚠ Avertissement :
La valeur de cette propriété est un remplacement sans base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sandbox.fields.check_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **faux** permet de contourner les restrictions ACL, ce qui pourrait exposer des données sensibles.
Dépendances et prérequis	Aucun

Appliquer l'utilisation d'alias d'informations d'identification [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]

Découvrez comment protéger vos informations d'identification contre toute utilisation non autorisée en configurant la propriété de Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le serveur MID (Management, Instrumentation, and Discovery) est une application Java qui s'exécute en tant que service Windows ou démon UNIX sur votre réseau local. Les propriétés de Serveur MID sont répertoriées dans la table [ecc_agent_property]. Vous pouvez y accéder dans votre instance en accédant à **Serveur MID** > **Propriétés**. Les alias d'informations d'identification permettent à un administrateur d'utiliser des informations d'identification spécifiques sur les calendriers Discovery. Les alias d'informations d'identification offrent un contrôle plus précis sur les informations d'identification qu'une table Découverte est autorisée à utiliser. Pour remédier à cette vulnérabilité de sécurité, définissez la valeur *alias_filtering_behavior* sur strict pour éviter une exposition inutile des informations d'identification avec des privilèges élevés. Reportez-vous à la rubrique MID Server properties pour en savoir plus.

En savoir plus

Attribut	Description
Nom de la configuration	*alias_filtering_behavior*
Type de configuration	Propriétés de Serveur MID (/ecc_agent_property_list.do)
Type de données	chaîne
Valeur recommandée	strict
Valeur par défaut	lâche
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2 • Score CVSS : faible • Détails du risque de sécurité : lorsque ce paramètre de sécurisation renforcée n'est pas défini sur strict, toutes les informations d'identification sont utilisées, quel que soit leur alias, pour les tables Découverte, ce qui augmente le risque d'accès non autorisé.
Dépendances et prérequis	Aucun
Références	• MID Server • Alias d'informations d'identification pour Découverte

Appliquer les ACL de type GroupBy

Configurez votre instance pour effectuer des vérifications d'ACL sur les colonnes groupées.

Utilisez la *glide.security.groupby_acl_check* propriété système pour configurer votre instance afin d'effectuer des vérifications ACL sur les colonnes groupées. Si cette propriété est définie sur la valeur recommandée **true**, les ACL des colonnes groupby sont respectées par défaut. L'attribut d'une *groupby_acl_check* table a priorité sur la *glide.security.groupby_acl_check* propriété. Si la propriété est définie sur **faux**, assurez-vous que l'attribut *groupby_acl_check* est défini sur **vrai** pour toute table qui doit avoir des vérifications ACL sur les colonnes groupées.

Assurez-vous que la propriété *glide.security.groupby_acl_check* est définie sur **true**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.groupby_acl_check`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : définir cette propriété sur **faux** désactivera la vérification des ACL sur les colonnes groupby, ce qui pourrait entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

Assurez-vous que les ACL de table d'archivage sont vérifiées [Nouveau dans Security Center 1.3 et mis à jour dans 1.5]

La `glide.security.enable_archive_table_acls` propriété contrôle si les listes de contrôle d'accès (ACL) de la table d'origine, la table à partir de laquelle la table d'archivage a été créée, sont évaluées sur faux.

La `glide.security.enable_archive_table_acls` propriété ne doit pas être définie sur faux, car les ACL de la table d'origine seront évaluées quelle que soit sa valeur. Vous pouvez éviter des ACL supplémentaires pour une table d'archivage en ne les ajoutant pas.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.enable_archive_table_acls`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3 • Score CVSS : faible • Détails du risque de sécurité : si la propriété est définie sur faux, les ACL ajoutées aux tables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	archivées sont ignorées, une action qui est contre-intuitive et peut donc conduire à un contournement de l'autorisation.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, toutes les ACL de lecture actives des tables d'archivage sont honorées. Si aucune ACL de lecture active n'existe ou si la propriété est définie sur faux, celle de la table d'origine (table depuis laquelle les données ont été archivées) s'appliquera à la table d'archivage. **Remarque :** Seules les ACL de lecture sont prises en charge sur les tables d'archivage. Les autres opérations effectuées sur les tables d'archivage sont pilotées en interne par l'intermédiaire d'un gestionnaire d'accès.

S'assurer que la création/la suppression des tableaux de bord nécessite une vérification d'accès [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]

La `glide.processors.check_access_before_process` propriété système active l'application de la liste de contrôle d'accès (ACL) pour la création ou la suppression de tableaux de bord lorsqu'un utilisateur est connecté.

Définissez la propriété système `glide.processors.check_access_before_process` sur **true**. Si la propriété n'apparaît pas dans la table Propriétés système [sys_properties], la valeur de secours est **définie sur vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.processors.check_access_before_process`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Valeur de secours	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : désactiver cette propriété en la définissant sur faux permet d'éviter les ACL sur les tableaux de bord. Cela permet

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	à tous les utilisateurs authentifiés avec peu de privilèges de supprimer et d'ajouter des tableaux de bord.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété contrôle la possibilité de créer de nouveaux sys_dashboards et de supprimer des tableaux de bord existants lorsqu'un utilisateur ne dispose pas des droits d'accès nécessaires. Lorsque la valeur est définie sur faux, les utilisateurs ayant des rôles inappropriés peuvent ajouter et supprimer des entrées sys_dashboard (bien que la couche GlideRecord doive revérifier les ACL existantes). Une valeur définie sur vrai limite les opérations d'ajout et de suppression pour les utilisateurs ne disposant pas des droits d'accès requis.

Exclure les tables et champs sensibles de la génération de données [nouveau dans Security Center 7.0]

Utilisez les propriétés système pour exclure les tables et les champs de la génération de données, qui est utilisée pour générer de faux ensembles de données basés sur des données existantes. Les tables et les champs ajoutés à ces listes d'exclusion ne peuvent pas être utilisés pour la fonctionnalité de génération de données.

Les tables incluses dans la propriété système sont exclues de la *glide.data.generation.excluded.tables* génération de données en plus des tables de métadonnées.

Les champs inclus dans une liste *glide.data.generation.excluded.fields.<TABLE-NAME>* séparée par des virgules pour sont exclus de la génération de données en plus de ces champs, le cas échéant :

- Numéro
- roles
- sys_class_name
- sys_created_by
- sys_id
- sys_mod_count
- sys_tags
- sys_updated_by

Passez en revue la liste des tables incluses dans la propriété *glide.data.generation.excluded.tables*. Ajoutez toutes les tables qui doivent être exclues de la génération de données à la liste de tables séparées par des virgules. En outre, les tables de métadonnées seront ignorées pour la génération de données.

Passez en revue la liste des champs de chaque table en examinant les propriétés au format : glide.data.generation.excluded.fields.<TABLE-NAME>. Ajoutez tous les champs sensibles pour la table spécifiée sous forme de liste de valeurs séparées par des virgules.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	• `glide.data.generation.excluded.tables` • `glide.data.generation.excluded.fields.*`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	• Liste de noms de tables séparés par des virgules • Liste de champs séparés par des virgules pour une table donnée
Valeur recommandée	• Liste de noms de tables séparés par des virgules qui doivent être exclus de la génération de données • Liste de noms de champs séparés par des virgules à exclure de la génération de données pour chaque table applicable
Valeur par défaut	"",""
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,6 • Score CVSS : faible • Détails du risque de sécurité : les données des tables utilisées dans la fonctionnalité de génération de données peuvent avoir des valeurs réelles ou fausses renseignées comme prévu par la fonctionnalité. Les valeurs sensibles des tables qui ne doivent pas être visibles ou répliquées peuvent être révélées à d'autres utilisateurs de l'instance.
Dépendances et prérequis	Le module d'extension de génération de données est en cours d'utilisation

Traduction automatique

Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour activer la validation stricte du `glide.security.csrf.strict.validation.mode` jeton CSRF. Si le jeton CSRF ne correspond pas, une nouvelle soumission de la demande est impossible.

Cette propriété empêche les utilisateurs d'accepter un avertissement qui permet d'envoyer une demande potentiellement malveillante à l'instance. Cet avertissement s'affiche lorsqu'une requête POST échoue en raison d'un jeton anti-CSRF qui ne correspond pas et qui appartient à l'une des autres sessions actives de la victime. S'il `glide.security.csrf.strict.validation.mode` n'est pas défini sur la valeur recommandée true, un attaquant peut formuler une attaque CSRF en utilisant un jeton anti-CSRF d'une autre session active appartenant à la victime. Une demande POST à

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une instance contient un jeton anti-CSRF dans « sysparm_ck » ou « X-UserToken » qui correspond à la session actuelle de l'utilisateur.

Si le jeton anti-CSRF est plutôt lié à l'une des autres sessions actives de l'utilisateur, la demande POST renvoie une redirection 302 vers security_interceptor.do avec un bouton Continuer disponible pour l'utilisateur lorsque cette propriété est définie sur faux. Cliquer sur ce bouton soumet à nouveau la demande à l'instance, sauf qu'elle dispose désormais d'un jeton anti-CSRF valide. Lorsque cette propriété est définie sur vrai, la redirection 302 vers la page security_interceptor.do n'affiche pas de bouton Continuer et l'utilisateur n'est pas autorisé à soumettre à nouveau la demande. Une attaque CSRF réussie permettra à un attaquant d'effectuer efficacement n'importe quelle opération que la victime est capable d'effectuer.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.csrf.strict.validation.mode`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour appliquer une validation stricte du jeton CSRF et empêcher sa réutilisation.
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	(Moyen) La contrefaçon de requête intersite constitue un risque de sécurité important qui viole l'intégrité des données d'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une demande mal formée à l'instance au nom de l'attaquant.
Cote de risque de sécurité	3.7
Impact fonctionnel	Cette correction active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Il vérifie si le jeton CSRF actuel a été utilisé précédemment. Si oui, cela empêche la soumission d'autres demandes d'écriture.
Risque de sécurité	(Moyen) La contrefaçon de requête intersite constitue un risque de sécurité important qui viole l'intégrité des données d'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une demande mal formée à l'instance au nom de l'attaquant.

Revenir à Configurer et charger la clé fournie par le client pour charger votre clé emballée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l'accès en lecture des développeurs délégués [Mis à jour dans Centre de sécurité 1.3]

S'il `com.glide.dd_allow_global_access_tables` ne contient pas la valeur recommandée de wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget et sp_page, ces tables peuvent être lues par un développeur délégué. Cela peut fournir au développeur délégué un accès en lecture à des informations sensibles.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.dd_allow_global_access_tables`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Valeur par défaut	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : assurez-vous que `com.glide.dd_allow_global_access_tables` est défini sur wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget sp_page.

Exiger la vérification de l'ACL AJAXGlideRecord [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour valider la `glide.script.secure.ajaxgliderecord` règle de contrôle d'accès (ACL) lorsque l'accès aux enregistrements côté serveur, tels que les tables, se fait à l'aide d'API GlideAjax à l'intérieur d'un script client.

Depuis les scripts clients, il est possible d'interroger des données arbitraires du serveur à l'aide de la fonction AJAXGlideRecord (GlideAjax -Client), à l'aide d'une syntaxe telle qu'un enregistrement Glide côté serveur. Il s'agit d'un outil puissant et utile dans de nombreux déploiements.

Si vous choisissez d'appliquer des listes de contrôle d'accès (ACL) aux appels d'API GlideAjax, vous ne pouvez interroger que les données auxquelles l'utilisateur actuellement connecté a accès. Par exemple, si un utilisateur ESS qui n'a pas le droit de lire la table cmn_location est connecté, tout appel d'API GlideAjax à cette table échouera.

Si l'API s'exécute ServiceNow AI Platform sans vérification des appels GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez GlideRecordSecure lors de l'interrogation des données pour garantir le niveau de sécurité le plus élevé. GlideRecord s'appuie sur l'application des ACL par le biais de configurations, tandis que GlideRecordSecure applique des contrôles de sécurité plus stricts. GlideRecordSecure offre une solution plus sécurisée et prête à l'emploi pour le traitement des données sensibles.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script.secure.ajaxgliderecord`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées, même lorsque les enregistrements sont accessibles via des API côté client.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.1
Impact fonctionnel	Cette correction applique la relation ACL avec les enregistrements côté serveur lorsque les demandes sont effectuées à l'aide des appels d'API AJAXGlideRecord. Si la configuration ACL n'est pas correctement configurée, cela peut avoir un impact. Pour plus de détails sur son impact et sur la manière de l'identifier, consultez l'article Audit et examen des transactions GlideRecord côté client (AJAXGlideRecord) [KB0550828] dans la section HI Base de connaissances .
Risque de sécurité	(Élevé) Grâce aux scripts clients, il est possible d'interroger des données arbitraires du serveur via l'API GlideAjax. Les ressources côté serveur sont accessibles sans autorisation appropriée. L'utilisation de la validation ACL aide donc l'application à valider la demande en fonction de l'autorisation configurée.
Solution de contournement	Assurez-vous que les ACL appropriées sont créées pour les includes de script, les processeurs et les autres entités utilisées par une API GlideAjax (AJAXGlideRecord) afin qu'elle s'exécute sous l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`, `canWrite()`, `canCreate()` et `canDelete ()` pour effectuer une autorisation utilisateur avant d'accéder aux enregistrements de table à l'aide de GlideRecord. Une autre méthode consiste à utiliser GlideRecordSecure. La classe est héritée du serveur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	GlideRecord qui exécute les mêmes fonctions que GlideRecord et applique également les ACL.
Références	Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client) Cette propriété appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution de scripts provenant du client, telles que `glide.script.allow.ajaxevaluate`. Pour plus d'informations, consultez Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès en écriture aux champs système pour les utilisateurs administrateurs [nouveau dans Security Center 7.0]

Utilisez la propriété système pour contrôler l'accès `glide.rest.table_api.admin_only_sys_fields` en écriture aux champs générés par le système.

La `glide.rest.table_api.admin_only_sys_fields` propriété contrôle l'accès en écriture à ces champs :

- sys_id
- sys_created_by
- sys_created_on
- sys_updated_by
- sys_updated_on

Lorsque cette propriété est définie sur **vrai**, seul un administrateur peut écrire dans ces champs qui sont des valeurs générées par le système. Lorsque la propriété est définie sur **false** ou qu'elle n'existe pas dans la table Propriétés système [sys_properties], les utilisateurs qui disposent d'un accès en création ou en écriture à une table peuvent écrire sur ces valeurs système à l'aide du Table API .

Définissez la propriété `glide.rest.table_api.admin_only_sys_fields` sur **vrai** pour empêcher les utilisateurs non-administrateurs de mettre à jour les champs système sur les enregistrements.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.rest.table_api.admin_only_sys_fields`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur de secours	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Les utilisateurs sans rôle administrateur peuvent mettre à jour des champs tels que sys_created_by ou sys_updated_on. Cet accès peut avoir un impact sur l'intégrité des métadonnées d'enregistrement créées ou mises à jour, donnant l'impression que les enregistrements ont été créés par un autre utilisateur ou mis à jour à un autre moment.
Impact fonctionnel	Toutes les intégrations ou les utilisateurs sans rôle administrateur qui utilisent l'API de table pour créer ou mettre à jour des enregistrements et modifier ces champs sont impactés. Ces demandes à l'API de table définissent le paramètre *`sysparm_suppress_auto_sys_field`* de requête sur **faux** et définissent ces champs dans le corps de la demande.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger l'approbation pour les changements d'appartenances aux groupes Office 365 basés sur des agents [Nouveau dans Security Center 7.0]

Activez le flux d'approbation pour ajouter ou supprimer des membres du groupe Office 365 via l'Agent IA d'appartenance au groupe Microsoft 365 à l'aide d'une propriété système.

Utilisez la *`sn_itsm_aia.office_365_group_member_approval.required`* propriété système pour contrôler si le flux d'approbation pour l'ajout ou la suppression de membres du groupe Office 365 via l'agent IA est activé ou désactivé. Lorsque le workflow d'approbation est activé, un enregistrement d'approbation doit être défini sur Approuvé par un membre du groupe spécifié dans la *`sn_itsm_aia.office_365_group_member_approval.group_id`* propriété système. Si la *`sn_itsm_aia.office_365_group_member_approval.group_id`* propriété n'est pas configurée, le *`Microsoft 365 group member approvers`* groupe est utilisé.

En savoir plus

Attribut	Description
Nom de la configuration	*`sn_itsm_aia.office_365_group_member_approval.required`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur de secours	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,9 • Score CVSS : moyen • Tout utilisateur qui peut accéder à l'Agent IA d'appartenance au groupe Microsoft 365 peut ajouter et supprimer des membres du groupe Office 365 du groupe Azure AD si l'approbation explicite du groupe d'approbateurs spécifié n'est pas requise. Assurez-vous que ces changements sont approuvés pour réduire le risque d'élévation du privilège en ajoutant ou en supprimant des membres sans autorisation appropriée.
Impact fonctionnel	Lorsque *sn_itsm_aia.office_365_group_member_approval.required* cette option est définie sur **vrai**, un membre du groupe spécifié dans *sn_itsm_aia.office_365_group_member_approval.<group_id>* doit approuver l'incident demandant l'ajout ou la suppression de membres du groupe Office 365. Si *sn_itsm_aia.office_365_group_member_approval.required* cette option est définie sur **faux** , aucune approbation n'est requise et l'agent IA peut gérer de manière autonome le processus d'ajout ou de suppression de membres d'un groupe Office 365.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Empêcher l'emprunt d'identité de l'utilisateur d'afficher les données de l'application

Utilisez les propriétés système pour empêcher un utilisateur empruntant l'identité de visualiser les données de l'application.

Empêchez le niveau administrateur d'accéder aux données spécifiques de l'application appartenant à cet utilisateur lorsqu'il emprunte l'identité d'un compte. Cette autorisation peut être définie au niveau de l'application en créant une propriété système spécifique à l'application.

Ces propriétés système utilisent le format de *<scope>.impersonateCheck* dénomination (par exemple *sn_hr_core.impersonateCheck*). Créez une propriété système avec la valeur **vrai** pour empêcher les utilisateurs d'accéder aux données spécifiques à l'application appartenant à un autre utilisateur lorsqu'ils empruntent l'identité d'un compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Toutes les applications ne sont pas conçues pour fonctionner dans cette configuration ou n'ont pas d'enregistrement Propriétés système [sys_properties] à cette fin. Les champs d'application suivants sont configurés pour fonctionner avec cette propriété.

- sn_opp_market
- sn_jny
- sn_imt_vaccine
- sn_imt_health_test
- sn_hr_core
- sn_egd_goals
- sn_egd_core
- sn_egd_act
- sn_em
- sn_talent_aia

Pour chaque application dont la *<scope>.impersonateCheck* propriété se trouve dans la table Propriétés système [sys_properties], assurez-vous que la valeur de la propriété est définie sur **true**.

Remarque :
Ces propriétés ne peuvent être modifiées que par l'administrateur du champ d'application pour l'application spécifique.

Utilisez ce script pour identifier les propriétés qui doivent être mises à jour ou créées sur l'instance :

```
var properties = [
   'sn_opp_market.impersonateCheck',
   'sn_jny.impersonateCheck',
   'sn_imt_vaccine.impersonateCheck',
   'sn_imt_health_test.impersonateCheck',
   'sn_hr_core.impersonateCheck',
   'sn_egd_goals.impersonateCheck',
   'sn_egd_core.impersonateCheck',
   'sn_egd_act.impersonateCheck',
'sn_em.impersonateCheck',
'sn_talent_aia.impersonateCheck'
];

var pm = new GlidePluginManager();

for (var i = 0; i < properties.length; i++) {
   var property = properties[i];
   var application = property.split('.')[0];
   var propertyValue = gs.getProperty(property, 'false');

   if (pm.isActive(application) && propertyValue.toLowerCase() != 'true') {
      gs.print(property);
   }
}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	*<scope>.impersonateCheck*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,8 • Score CVSS : faible • Une valeur **définie sur faux** pour ces propriétés permet à un utilisateur de niveau administrateur d'emprunter l'identité d'un autre utilisateur et d'accéder aux données de l'application avec l'accès de l'utilisateur dont l'identité a été empruntée. Cela peut être indésirable ou permettre un accès non autorisé aux données dans des contextes d'application spécifiques.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Renforcer la validation des paramètres de l'état OAuth

Configurez la*glide.oauth.state.parameter.required* propriété pour empêcher votre instance contre les attaques de contrefaçon de requête de site à site (CSRF).

La *glide.oauth.state.parameter.required* propriété permet d'exiger le paramètre État dans une demande OAuth pour le flux de code d'autorisation. Le paramètre State est une valeur de chaîne qui ne doit pas contenir de caractères spéciaux ni être vide. Définir cette propriété sur **vrai** garantit qu'un attaquant ne peut pas effectuer d'attaques de contrefaçon de requête de site à site (CSRF) pendant l'authentification, ce qui protège votre instance contre les attaques d'un utilisateur dont l'identité a été empruntée.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.oauth.state.parameter.required*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : définissez cette propriété sur **vrai** pour vous assurer que les attaques CSRF sont évitées.
Dépendances et prérequis	Aucun

Appliquer des règles strictes pour le téléchargement d'images par l'utilisateur

Utilisez la propriété pour activer le `glide.security.strict.user_image_upload` contrôle d'accès pour le chargement/la mise à jour d'une photo de profil lorsqu'il est effectué sur un enregistrement utilisateur.

Ce paramètre ouvre la possibilité qu'un utilisateur non autorisé télécharge une image sur le profil d'un autre utilisateur.

- Lorsque vous définissez cette propriété sur **vrai**, les ACL de table sont appliquées lors du chargement de photos, ce qui permet uniquement aux utilisateurs autorisés de charger une image.
- Lorsque vous le définissez sur **false**, les ACL ne sont pas appliquées aux chargements d'images dans le champ Photo.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.strict.user_image_upload`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour limiter le chargement de l'image de l'utilisateur aux seuls utilisateurs autorisés.
Valeur recommandée	vrai
Cote de risque de sécurité	3.7
Impact fonctionnel	Aucun impact sur les fonctionnalités, car les utilisateurs autorisés peuvent toujours télécharger des images sur leur profil d'utilisateur.
Risque de sécurité	(Faible) Lorsque vous définissez cette propriété sur **false**, un utilisateur authentifié peut charger une image sur le compte d'un autre utilisateur sans autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre les domaines de messagerie pour l'inscription des utilisateurs externes [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]

Utilisez la propriété pour répertorier les domaines d'e-mail *sn_ext_usr_reg.allowed_email_domains* externes acceptables.

La propriété système **sn_ext_usr_reg.allowed_email_domains** définit les adresses e-mail autorisées à s'auto-enregistrer sur une ServiceNow instance. Le format doit être une liste de domaines d'e-mail acceptables séparés par des virgules, tels que domain1.com domain2.com où des e-mails tels que example@domain2.com seront acceptés. Si **sn_ext_usr_reg.allowed_email_domains** n'est pas défini avec une liste de domaines acceptables, les utilisateurs avec n'importe quelle adresse e-mail sont autorisés à enregistrer des comptes sur les instances. Si cette propriété n'est pas définie, les acteurs malveillants peuvent effectuer l'enregistrement à l'aide d'adresses e-mail de domaines indésirables pour obtenir un accès authentifié à l'instance.

En savoir plus

Attribut	Description
Nom de la propriété	*sn_ext_usr_reg.allowed_email_domains*
Type de configuration	Propriétés système (/sys_properties_list.do), Propriétés des communautés
Catégorie	Contrôle d'accès
Objectif	Répertoriez les domaines d'e-mail pour autoriser l'e-mail de l'utilisateur pour l'inscription.
Valeur recommandée	Définir comme une valeur non vide
Type de configuration	Chaîne
Risque de sécurité	(Élevé) Les acteurs malveillants pourraient effectuer l'enregistrement à l'aide d'adresses e-mail de domaines indésirables. Assurez-vous que **sn_ext_usr_reg.allowed_email_domains** n'est pas défini sur une valeur vide.
Cote de risque de sécurité	7.5
Références	Communities

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3]

Lorsque vous activez le module d'extension de haute sécurité, ce dernier crée ou met à jour des centaines de configurations différentes pour contrôler le niveau de sécurité de votre instance. Ces configurations atténuent la plupart des attaques OWASP les plus fréquentes en activant un contrôle d'accès strict, la validation d'entrée et l'encodage de sortie.

Ces configurations comprennent :

- Contrôle d'accès
- Règles métier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Propriétés système
- Action de politique d’interface utilisateur
- Actions des scripts
- Includes de script

Exemple

Reportez-vous aux exemples pour les propriétés suivantes :

Propriété	Sujet
glide.ui.escape_all_script	Script Jelly d’échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]
glide.security.strict.actions	Vérifier les conditions de l’action de l’interface utilisateur avant son exécution
glide.security.csrf_previous.autoriser	Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]
glide.security.csrf.strict.validation.mode	Empêcher les utilisateurs d’accepter l’avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.high_security
Type de configuration	Définition du système > Modules d’extension : Développement
Catégorie	Contrôle d'accès
Objectif	Il est obligatoire d’activer ce module d’extension. Il augmente le niveau de sécurité d’une instance, ce qui réduit la surface d’attaque en atténuant les 10 premières attaques de l’OWASP, notamment CSRF, XSS, les cookies de session de sécurisation et les téléchargements de fichiers.
Valeur recommandée	Actif
Cote de risque de sécurité	9.8
Impact fonctionnel	Ce module d'extension active plusieurs configurations de sécurité de système, qui peuvent également avoir un impact sur l'interface utilisateur et les fonctionnalités.
Risque de sécurité	(Élevé) De nombreuses configurations de sécurité sont involontairement laissées ouvertes, ce qui peut ouvrir la porte à certaines vulnérabilités critiques.
Références	Activation des paramètres de sécurité élevée Paramètres de sécurité élevée

Pour en savoir plus sur l’activation d’un module d’extension, consultez Activate a plugin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Respecter les ACL de remplacement de l'administrateur

La `glide.security.admin.override.accessterm` propriété contrôle les administrateurs pour qu'ils ne puissent pas remplacer l'évaluation d'ACL, même lorsque le remplacement doit être effectué.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.admin.override.accessterm`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Contrôle l'impossibilité pour les administrateurs de remplacer l'évaluation d'ACL.
Type de données	Booléen
Valeur recommandée	Vrai
Valeur par défaut	Vrai
Risque de sécurité	(Faible) Les ACL sont évaluées de façon cumulative. S'il existe un certain nombre d'ACL sur un champ donné et que l'option Remplacements administrateur est définie sur faux (non sélectionné), les remplacements administrateur effectifs pour toutes les ACL sont considérés comme faux.
Cote de risque de sécurité	3.8
Références	Règles de la liste de contrôles d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Empêcher les utilisateurs inactifs de se connecter [nouveau dans le centre de sécurité 1.5]

Configurez cette propriété pour contrôler si les utilisateurs inactifs peuvent s'authentifier sur votre instance.

Définissez la valeur de la `glide.authenticate.only.allow.active.user.login` propriété sur vrai (recommandé), cela garantit que les utilisateurs de la table sys_user marqués comme inactifs ne peuvent pas se connecter à l'instance et sont verrouillés.

Si le paramètre est configuré sur faux, les utilisateurs peuvent toujours accéder à l'instance et aux données auxquelles ils avaient précédemment accès.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.only.allow.active.user.login`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée vrai peut permettre aux utilisateurs inactifs comme un employé licencié de toujours avoir accès à l'instance et à toutes les données.
Dépendances et prérequis	Aucun

Empêcher l'accès non authentifié au client Web incorporé de l'agent virtuel

Découvrez comment configurer la table pour empêcher les *sn_va_web_client_app_embed* utilisateurs non authentifiés d'accéder aux clients Web intégrés.

La page d'interface utilisateur, *sn_va_web_client_app_embed*qui est un client Web intégré pour Agent virtuel, contient les listes de contrôle d'accès (ACL) marquées comme vraies dans la table sys_public prête à l'emploi. Il a été confirmé qu'il existe des cas d'utilisation où l'accessibilité publique est nécessaire, mais il ne s'agit pas d'une norme pour la définir par défaut comme accessible au public.

Si le client Web intégré n'est pas nécessaire pour les utilisateurs non authentifiés, ouvrez l'enregistrement *sn_va_web_client_app_embed* (sys_id 04b1905473222300e985658b4cf6a7ef) dans la table Pages publiques [sys_public] et désélectionnez le champ **Actif** pour désactiver la page.

En savoir plus

Attribut	Description
Nom de la configuration	**sn_va_web_client_app_embed**
Type de configuration	Page de l'interface utilisateur (sys_ui_page_list.do)
Type de données	Table
Valeur recommandée	La page publique **sn_va_web_client_app_embed** [sys_public] (sys_id 04b1905473222300e985658b4cf6a7ef) n'existe pas ou n'est pas active.
Valeur par défaut	Non disponible (il s'agit d'une valeur de table)
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : il est recommandé de désactiver la page de l'interface utilisateur,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	*sn_va_web_client_app_embed*si un client Web intégré n'est pas nécessaire pour les utilisateurs non authentifiés.
Dépendances et prérequis	Aucun

Restreindre les demandes JSONP aux URL approuvées [Mis à jour dans Centre de sécurité 1.3]

Spécifiez des URL fiables pour le service de $http AngularJS afin d'autoriser ou de rejeter les demandes JSONP.

Augmentez la sécurité sur votre instance en vous assurant que seules les URL approuvées pour le service de $http AngularJS peuvent autoriser/rejeter des demandes JSONP. Les demandes JSONP sont autorisées pour n'importe quelle URL si ces propriétés ne sont pas configurées et activées.

Utilisez la valeur de la propriété système **angular.jsonp.inclusion_list.urls** pour définir une liste d'URL fiables et autorisées à cette fin. Définissez la valeur de la propriété système **angular.jsonp.inclusion_list.enabled** sur **true** pour limiter le JSONP autorisé aux URL répertoriées dans **angular.jsonp.inclusion_list.urls**.

En savoir plus

Attribut	Description
Nom de la configuration	*angular.jsonp.inclusion_list.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : moyenne • Score CVSS : 5,4 • Détails du risque de sécurité : si vous définissez cette propriété sur **faux** , les demandes JSONP s'appliquent à n'importe quelle URL.
Dépendances et prérequis	Aucun

Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF

Réduisez le risque de contrefaçon de requête intersite (CSRF) en empêchant les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF.

Activez la validation stricte des jetons CSRF pour empêcher la réutilisation des jetons de contrefaçon de requête intersite (CSRF), ce qui peut entraîner des attaques CSRF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez la valeur de propriété système **glide.security.csrf.strict.validation.mode** sur **vrai** pour activer la validation stricte du jeton CSRF. Si cette propriété n'existe pas dans votre table Propriétés système [sys_properties], la valeur par défaut est **vrai** à partir de Xanadu.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.security.csrf.strict.validation.mode
Applicabilité du module d'extension	Aucun
Risque de sécurité	La contrefaçon de requête intersite constitue un risque de sécurité important qui viole l'intégrité des données d'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une demande mal formée à l'instance au nom de l'attaquant.
Score du système de notation des vulnérabilités courantes (CVSS)	3.7
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Cette correction active une étape de validation supplémentaire avant que l'utilisateur n'envoie une demande d'écriture à l'instance. Il vérifie si le jeton CSRF actuel a été utilisé précédemment. Si c'est le cas, cela empêche la soumission d'autres demandes d'écriture.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	vrai
Valeur de secours	vrai
Valeur recommandée	vrai

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'exécution de requêtes de base de données brutes [Mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]

Contrôlez si un utilisateur peut effectuer des requêtes SQL brutes sur la base de données.

Cette`glide.db.allow_unsafe_dbi_execute_sql` propriété permet aux utilisateurs d'effectuer des requêtes SQL brutes sur la base de données, ce qui peut donner accès à des tables et à des données en dehors des restrictions GlideRecord. Si cette propriété n'est pas définie sur la valeur recommandée de `false`, cela permet d'appeler `dbi.executeStatement()` à partir d'un script Glide, ce qui peut entraîner l'exécution d'instructions SQL malveillantes.

⚠ Avertissement :
Cette propriété est à la fois sûre et ne remplace pas de base de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.db.allow_unsafe_dbi_execute_sql`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : ne pas définir cette propriété sur **faux** permet d'appeler à partir d'un `dbi.executeStatement()` script Glide.
Dépendances et prérequis	Aucun
Références	Règles de la liste de contrôles d'accès

Masquer les commentaires des utilisateurs sur les articles [nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler si les `glide.knowman.show_user_feedback` commentaires des commentaires sont visibles.

Si `glide.knowman.show_user_feedback` cette option n'est pas définie sur jamais, les commentaires des utilisateurs ayant des rôles définis dans la propriété Glide seront visibles sur les articles de la base de connaissances. `glide.knowman.show_user_feedback.roles` Étant donné que les commentaires des commentaires peuvent contenir des informations sensibles, il est possible que vous ne souhaitiez pas qu'ils soient visibles. Si cette propriété n'est pas définie sur jamais, il pourrait y avoir des impacts sur la confidentialité si des informations sensibles sont divulguées dans les commentaires.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.knowman.show_user_feedback`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	liste de choix
Valeur recommandée	jamais
Valeur par défaut	onload
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : ne pas définir cette propriété sur jamais peut entraîner la divulgation d'informations sensibles dans les commentaires des commentaires.
Dépendances et prérequis	Aucun
Impact fonctionnel	Affiche les commentaires des utilisateurs sur les articles de la base de connaissances en fonction des choix mentionnés dans la configuration.

Exiger l'authentification par défaut pour les includes de script appelables par le client [Mis à jour dans Centre de sécurité 1.3]

Par défaut, les includes de script appelables par le client qui ne définissent pas explicitement la visibilité sont publics. Si nécessaire, ajoutez la propriété pour activer le `glide.script.ccsi.ispublic` contrôle de la confidentialité sur tous les includes de script appelables par le client accessibles via des pages publiques.

Lorsque vous ajoutez cette propriété, vous devez définir sa valeur sur **false**, ce qui signifie que tous les includes de script pouvant être appelés par les clients sont privés et modifie leur visibilité dans les pages publiques.

Remarque :
Vous ne pouvez pas ajouter la propriété avec la valeur **vrai** ou changer sa valeur de **faux** à **vrai**. Si vous tentez de le faire, un message d'erreur s'affiche.

Si nécessaire, vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction isPublic( ).

- Le paramètre isPublic() est prioritaire sur la `glide.script.ccsi.ispublic` propriété.
- Par exemple, si vous définissez isPublic() sur **true** dans un script individuel, il le rend public, ce qui remplace la propriété qui rend privés tous les autres includes de script pouvant être appelés par un `glide.script.ccsi.ispublic` client.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script.ccsi.ispublic`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Le fait de rendre les includes de script appelables par le client privés signifie que les invités qui accèdent aux pages publiques ne peuvent pas accéder à l'include de script pouvant être appelé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	par le client. Un utilisateur non connecté ne peut pas exécuter un script privé.
Valeur recommandée	Faux
Valeur par défaut	Faux
Cote de risque de sécurité	7.5
Impact fonctionnel	Si les includes de script appelables par le client sont désignés comme publics (c'est-à-dire que cette propriété est manquante), les utilisateurs non authentifiés peuvent exécuter des scripts clients. Ajouter la propriété restreint l'exécution de scripts par un utilisateur non connecté.
Risque de sécurité	(Élevé) Si vous n'ajoutez pas cette propriété, le script côté client inclut les ACL contournables, ce qui peut entraîner des fonctionnalités publiques non prévues. Si le script client fournit des informations confidentielles, il peut présenter un risque de sécurité potentiel défavorable.
Solution de contournement	Si vous définissez la propriété sur **faux**, tous les includes de script appelables par les *`glide.script.ccsi.ispublic`* clients deviennent privés. Vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction isPublic( ). La fonction isPublic a priorité sur la *`glide.script.ccsi.ispublic`* propriété. Ajoutez la syntaxe suivante à l'include de script : isPublic :function(){return[true/false] ;},

Appliquer le comportement de l'instance de production [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Configurez si votre instance doit être traitée comme une instance de production ou de non-production.

Si la *`glide.installation.production`* propriété n'est pas définie sur la valeur recommandée **true**, l'instance n'est pas traitée comme une instance de production, ce qui permet à zboot et à d'autres scripts potentiellement dangereux de s'exécuter. Permettre à une instance de production d'être évaluée comme une instance de non-production peut entraîner des fuites d'informations ou des attaques par déni de service (DoS).

En savoir plus

Attribut	Description
Nom de la configuration	*`glide.installation.production`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : si vous définissez cette valeur de propriété sur **faux** , l'instance est traitée comme une instance de non-production, ce qui permet l'exécution de zboot et d'autres scripts potentiellement dangereux.
Dépendances et prérequis	Aucun

Restreindre l'accès au script en arrière-plan [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Configurez la`glide.script_processor.admin` propriété pour définir le rôle requis pour accéder au module Arrière-plan de script.

Cette propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si `glide.script_processor.admin` elle n'est pas définie sur la valeur recommandée et par défaut administrateur, les utilisateurs ayant un rôle avec moins de privilèges seront en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela conduira à un contournement complet du système d'ACL permettant un accès complet aux tables.

Assurez-vous que la propriété `glide.script_processor.admin` est définie sur l'administrateur. Il s'agit de la valeur par défaut pour les instances.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.script_processor.admin`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	administrateur
Valeur par défaut	administrateur
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 8,8 • Score CVSS : élevé • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Administrateur permet à n'importe quel utilisateur d'exécuter des scripts en arrière-plan sur l'instance.
Dépendances et prérequis	Aucun

Restreindre l'accès aux e-mails dont la table cible est vide

Activez la propriété pour restreindre l'accès de l'utilisateur `glide.email.email_with_no_target_visible_to_all` aux e-mails, sauf s'il en est l'expéditeur ou qu'il possède un rôle administrateur.

Les utilisateurs non autorisés peuvent accéder aux e-mails de la table sys_email_list auxquels il manque un enregistrement cible. Au lieu d'appliquer des ACL sur les entrées d'e-mail, cette propriété restreint l'accès uniquement à l'expéditeur d'e-mail et aux utilisateurs disposant du rôle administrateur.

Remarque :
Les e-mails envoyés et reçus par l'instance s'affichent dans la table sys_email_list. Toutefois, seuls les e-mails reçus marqués avec un état Erreur et Ignoré doivent avoir une table cible vide.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.email_with_no_target_visible_to_all`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer	Contrôle d'accès
Objectif	Pour empêcher Client de messagerie d'afficher les e-mails lorsque l'utilisateur n'autorise pas l'accès.
Valeur recommandée	Faux
Valeur par défaut	vrai
Cote de risque de sécurité	6.5
Impact fonctionnel	Les utilisateurs ne sont plus en mesure de voir les e-mails dont la table cible est vide, sauf s'ils sont administrateurs ou qu'ils sont l'expéditeur de l'e-mail.
Risque de sécurité	(Modéré) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder à tous les e-mails dont le champ target_table est vide.
Références	Propriétés d'e-mail avancées https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l’accès aux module d’extension de plages d’adresses IP spécifiques [Mis à jour dans Centre de sécurité 1.3]

Utilisez le module d’extension pour restreindre l’accès `com.snc.ipauthenticator` à des plages IP spécifiques. À moins que l’accès public ne soit destiné à l’instance, les administrateurs doivent limiter l’accès aux blocs réseau IP qui leur sont affectés.

Prérequis

Lorsqu’il est défini sur vrai, ce module d’extension limite l’accès à des plages IP spécifiques. À moins que l’accès public ne soit destiné à l’instance, les administrateurs doivent limiter l’accès aux blocs réseau IP qui leur sont affectés. Une liste d’exclusion (refuser) ou une liste d’inclusion (Autoriser) d’adresses IP peut être créée via le contrôle d’accès à l’adresse IP (ip_access_list.do).

Avant de définir cette propriété, vous devez activer le module d’extension Authentification basée sur la plage IP (com.snc.ipauthenticator).`com.snc.ipauthenticator` Pour en savoir plus, consultez Authentification basée sur la plage IP et dans la section Étapes de configuration (ci-dessous).

Assurez-vous que le module d’extension `com.snc.ipauthenticator` est activé et qu’il existe au moins une politique d’accès IP active dans la table ip_access.

En savoir plus

Attribut	Description
Nom du module d'extension	• com.snc.ipauthenticator • ip_access
Type de configuration	Sécurité du système > contrôle d’accès à l’adresse IP
Catégorie	Contrôle d'accès
Objectif	Pour ajouter la plage d’adresses IP qui peuvent ou non accéder à l’instance aux listes de domaines approuvés et non approuvés.
Valeur recommandée	Actif
Valeur par défaut	Aucun. Il s’agit d’un module d’extension, pas d’une propriété de Glide ; Par conséquent, il n’y a pas de valeur par défaut.
Cote de risque de sécurité	5.3
Impact fonctionnel	Les plages IP refusées par le client sont utilisées pour cet élément de correction. Aucun impact, car le client définit la liste cible.
Risque de sécurité	(Faible) L’exposition inutile à l’instance cible sur Internet doit être limitée à l’aide de la fonctionnalité de contrôle d’accès IP.
Références	Authentification basée sur la plage IP

Étapes de configuration

1. Assurez-vous que le module d’extension com.snc.ipauthenticator est actif.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès à l'adresse IP**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Nouveau** pour créer une liste d'exclusion (refuser) ou une liste d'inclusion (Autoriser) d'adresses IP.
4. Cliquez sur **Envoyer**.

Restreindre l'accès aux bases de connaissances [nouveau dans Security Center 1.3]

Cette `glide.knowman.block_access_with_no_user_criteria` propriété est utilisée pour contrôler l'accès en lecture/écriture des utilisateurs sur les articles basés sur la base de connaissances.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.knowman.block_access_with_no_user_criteria`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 9,1 • Score CVSS : critique • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée vrai, tout utilisateur peut lire et contribuer à une base de connaissances.
Dépendances et prérequis	Aucun
Impact fonctionnel	Refuse l'accès à une base de connaissances lorsque Autorisation de lecture ou Autorisation de contribution n'est pas spécifiée.

Traduction automatique

Restreindre les autorisations pour le modèle CMDB [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété système pour limiter l'accès `csm_cmdb_model.customer_visible_flag` des clients aux données de la table Modèles de produits en tant que contrôle d'accès supplémentaire au modèle CMDB.

Définissez la `csm_cmdb_model.customer_visible_flag` propriété sur **vrai** pour activer le champ Visible par le client pour les tables répertoriées ci-dessous :

- Table Modèles de produits [cmdb_model]
- Table Modèles logiciels [cmdb_software_product_model]
- Table Modèles d'application [cmdb_application_product_model]
- Table des modèles de consommables [cmdb_consumable_product_model]

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Table Modèles d'installation [cmdb_facility_product_model]
- Table Modèles matériels [cmdb_hardware_product_model]

Si vous définissez cette propriété sur **vrai,** toutes les valeurs de cmdb_model sont masquées par défaut.

Définissez la propriété sur **faux** pour ne pas prendre en compte la colonne de customer_visible/atrribute sur la table cmdb_model et pour vous fier aux bases cmdb_model ACL qui sn_esm_user sont accessibles.

En savoir plus

Attribut	Description
Nom de la propriété	*csm_cmdb_model.customer_visible_flag*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Lorsque la valeur est définie sur**« vrai** », le système utilise le paramètre du champ Visible par le client pour déterminer l'accès aux données de modèle de produit sur le portail de service client.
Valeur recommandée	vrai
Valeur par défaut	Faux
Type de configuration	Booléen
Risque de sécurité	(Modéré) Tout utilisateur disposant du rôle sn_esm_user et des ACL prêtes à l'emploi peut avoir des autorisations pour le modèle CMDB. **Remarque :** ce rôle a tendance à être accordé aux utilisateurs externes. Les utilisateurs externes pourraient sans le vouloir recevoir des autorisations pour le modèle CMDB.
Références	Limiter l'accès aux données des modèles de produits sur le Customer Service Portal

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès non authentifié aux pièces jointes

Utilisez la *glide.image_provider.security_enabled* propriété pour contrôler les paramètres de sécurité des images. Si la valeur est définie sur **vrai**, les images ne sont visibles que par les utilisateurs authentifiés et autorisés. Si la valeur est définie sur **faux**, les images sont visibles par toute personne disposant d'une URL vers la pièce jointe.

Sécurisez les images sur votre instance pour éviter toute fuite d'informations sensibles. Les images de votre instance sont accessibles via des URL qui se terminent par .iix.

Définissez la propriété système **glide.image_provider.security_enabled** sur **vrai** pour empêcher l'accès à vos images via ces URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Cette propriété n'est pas respectée pour les images de la table des pièces jointes si la table d'origine est l'une des suivantes :

- Papeterie [sysevent_email_style]
- Sections de page d'accueil [sys_home]
- Propriétés système [sys_properties]

La restriction doit être appliquée aux utilisateurs non authentifiés, car certaines pièces jointes peuvent contenir des informations sensibles.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.image_provider.security_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour empêcher l'accès non authentifié à la pièce jointe lorsqu'elle est restituée à l'aide du format `.iix` .
Valeur recommandée	vrai
Valeur par défaut	Faux
Impact fonctionnel	Aucun impact significatif sur la fonctionnalité. L'expérience utilisateur peut être un peu affectée, car l'utilisateur qui accédait auparavant directement à .iix doit passer par l'authentification.
Risque de sécurité	• Score de gravité : 6,5 • Détails du risque de sécurité : la restriction doit être appliquée pour les utilisateurs non authentifiés, car certaines pièces jointes peuvent contenir des informations sensibles.
Références	Administration des pièces jointes Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès aux entrées de journal personnalisées [Mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]

Utilisez la `glide.live_feed.custom_journal.acl_check_enabled` propriété pour respecter les ACL sur les champs de journal personnalisés.

Si `glide.live_feed.custom_journal.acl_check_enabled` n'est pas défini sur la valeur recommandée vrai, tous les utilisateurs peuvent voir toutes les entrées de journal dans la fonctionnalité d'alimentation de vie. Définir la propriété sur vrai permet de respecter les ACL dans les champs de journal personnalisés, ce qui est une fonctionnalité intéressante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.live_feed.custom_journal.acl_check_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour contrôler quels utilisateurs voient quelles entrées de journal en fonction des ACL.
Valeur recommandée	vrai
Valeur par défaut	vrai
Type de configuration	Booléen.
Risque de sécurité	(Modéré) Lorsque la valeur est définie sur vrai, seules les entrées de journal personnalisées qui passent l'ACL s'affichent dans Flux en direct, sinon tous les utilisateurs peuvent voir toutes les entrées de journal.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès en lecture au contexte de flux [nouveau dans Security Center 1.5]

Utilisez la `com.snc.process_flow.reporting.require_flow_access` propriété pour appliquer si une vérification d'accès supplémentaire est requise pour qu'un utilisateur lise une vérification de flux.

Lorsque la `com.snc.process_flow.reporting.require_flow_access` propriété est définie sur la valeur recommandée vrai, une vérification d'accès supplémentaire est effectuée pour un utilisateur qui tente de lire un contexte de flux. Il peut y avoir une divulgation mineure d'informations si cette propriété est définie sur faux.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.process_flow.reporting.require_flow_access`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété est définie sur faux, son comportement existant est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	conservé. Si vous réglez cette propriété sur vrai, la couche de sécurité supplémentaire de l'accès en lecture est appliquée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est activée, la sécurité de lecture des enregistrements de contexte de flux est accrue. L'instance impose qu'un utilisateur essayant de lire le contexte de flux dispose également d'un accès en lecture au flux parent.

Restreindre l'emprunt d'identité à l'administrateur [nouveau dans Security Center 2.0]

La `glide.sys.permissive.impersonate` propriété peut être utilisée pour empêcher les rôles non-administrateurs d'emprunter l'identité d'autres utilisateurs.

Lorsque la `glide.sys.permissive.impersonate` propriété est définie sur faux, seuls les utilisateurs ayant le rôle administrateur peuvent emprunter l'identité d'autres utilisateurs. Lorsque cette propriété est définie sur vrai, les utilisateurs peuvent être en mesure d'utiliser des composants d'application qui exposent des API d'emprunt d'identité pour emprunter l'identité d'un utilisateur disposant de privilèges plus élevés. Cela peut entraîner un accès non autorisé si ces composants d'application sont mal configurés, car les utilisateurs non-administrateurs peuvent accéder à la fonctionnalité d'emprunt d'identité.

Vous pouvez définir la propriété sur la valeur autre que celle par défaut lorsque vous avez besoin que les utilisateurs non-administrateurs puissent emprunter l'identité d'autres utilisateurs.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sys.permissive.impersonate`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur la valeur recommandée faux, un utilisateur non-administrateur peut utiliser

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	des composants d'application qui exposent les API, ce qui lui permet d'emprunter l'identité d'un utilisateur disposant de privilèges plus élevés.
Dépendances et prérequis	Aucun
Impact fonctionnel	Les utilisateurs non-administrateurs peuvent accéder aux fonctionnalités d'emprunt d'identité avec certaines personnalisations pour d'autres scripts et pages de l'interface utilisateur. Cependant, il est essentiel de s'assurer que seuls les bons utilisateurs ont accès à ces fonctionnalités. **Remarque :** Quand `glide.sys.permissive.impersonate` cette option est définie sur vrai, les utilisateurs non-administrateurs ayant le rôle peuvent toujours emprunter l'identité `impersonate` .

Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) [Mis à jour dans Centre de sécurité 1.3]

Activez le module d'extension Security Jump Start (ACL Rules) (com.snc.system_security`com.snc.system_security`) pour créer plusieurs ACL importantes qui valident les contrôles d'accès sur certaines des tables clés du système dans .ServiceNow AI Platform

Ces règles permettent de démarrer rapidement la sécurisation de nombreuses tables système, ce qui facilite la mise en production d'une instance. Le module d'extension de démarrage rapide de la sécurité (règles ACL) est installé automatiquement sur toutes les nouvelles instances.

En savoir plus

Attribut	Description
ID de module d'extension	`com.snc.system_security`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Contrôle d'accès
Objectif	Activez le module d'extension de démarrage rapide de la sécurité (règles ACL) pour assurer la conformité de sécurité appropriée. Il fournit des ACL de base qui sécurisent les tables système en premier lieu au lieu de créer manuellement pour chaque table système fournie avec le provisionnement par défaut d'une instance. Ces ACL sont utiles lorsque l'instance nouvellement créée doit rapidement passer en production.
Valeur recommandée	Actif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	Aucun. Il s'agit d'un module d'extension, pas d'une propriété Glide, il n'y a donc pas de valeur par défaut. Le plugin est installé par défaut sur zBoot (reset).
Cote de risque de sécurité	8.1
Impact fonctionnel	L'installation de ce module d'extension sans audit des ACL existantes sur l'instance a un impact fonctionnel significatif. La sensibilisation et les définitions des clients sont nécessaires avant que la correction ne puisse avoir lieu.
Risque de sécurité	(Élevé) Le contrôle d'accès doit être appliqué pour verrouiller l'accès involontaire à l'instance. Les règles de démarrage rapide ACL ont été créées pour fournir un point de départ sur la sécurisation de nombreuses tables système afin de faciliter la mise en production rapide d'une entreprise.
Références	Démarrage rapide de la sécurité : règles ACL

Étapes de configuration

Si ce module d'extension n'est pas activé sur votre instance, contactez ServiceNow le support. L'activation du module d'extension à ce stade peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production. Si un administrateur est intéressé par les nouvelles règles ACL fournies par le module d'extension, vous pouvez en créer une ou plusieurs manuellement dans une instance existante si nécessaire. Cette liste d'ACL peut être utilisée comme ligne directrice dans ce cas.

Utilisation de l'opération multiple d'insertion sécurisée dans l'API de jeu d'importation [nouveau dans Security Center 1.3]

Utilisez la `com.glide.import_set_api.insert_multiple_optimize` propriété pour contrôler si `GlideRecordSecure` ou `GlideRecord` est utilisé pour l'opération Insertion multiple dans l'API de jeu d'importation.

Si `com.glide.import_set_api.insert_multiple_optimize` la valeur recommandée est faux, `GlideRecordSecure` est utilisé pour insérer des enregistrements et les listes de contrôle d'accès (ACL) au niveau de la table sont évaluées. Si cette propriété est définie sur vrai, `GlideRecord` est utilisé pour insérer des enregistrements et les ACL au niveau de la table ne sont pas évaluées ; En outre, vous devez vous assurer que l'ACL de point de terminaison REST multiple d'insertion d'API de jeu d'importation (sys_id : 3101b770ff2211105cf343d0653bf182) est active et que les utilisateurs ont le rôle, import_transformer.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.import_set_api.insert_multiple_optimize`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur faux, un utilisateur avec peu de privilèges peut insérer des données dans des tables en dehors du cadre de ses rôles privilégiés.
Comportement réversible	Remplacement sécurisé et Aucun remplacement de base de données.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété optimise les performances de l'API de jeu d'importation à l'aide de GlideRecord pour enregistrer les données. Lorsque le paramètre est défini, un utilisateur d'intégration doit disposer du rôle import_transformer pour accéder à l'API.
Références	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Appliquer la sécurité stricte des requêtes SOAP [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour renforcer la `glide.soap.strict_security` sécurité des services web.

Cette propriété utilise une combinaison de :

- Défi/réponse d'authentification de base sur le protocole HTTP et
- Contrôles d'accès au niveau du système dans le Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) [Mis à jour dans Centre de sécurité 1.3].

Si vous définissez cette propriété sur **vrai**, elle effectue les actions suivantes :

- Si l'utilisateur dispose du rôle approprié pour effectuer l'opération, il vérifie la demande SOAP entrante pour obtenir l'autorisation de rôle à valider. Elle se produit lors d'appels/de requêtes de service web SOAP effectués sur ServiceNow AI Platform des tables lors de l'exécution des opérations CRÉER, LIRE, METTRE À JOUR ou SUPPRIMER.
- Vérifie les ACL au niveau du système lors de la récupération des données sous forme de données SOAP sur la table.
- Vérifie les ACL au niveau du champ pour toute opération CRUD effectuée sur un champ de table.

Les vérifications ACL ne sont effectuées que pour les appels d'API de table standard et non pour les services web.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.soap.strict_security`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Valeur par défaut	vrai
Valeur recommandée	vrai
Impact fonctionnel	Cette correction applique le contrôle d'accès au niveau du système tout en récupérant les données des tables/pages sous la forme de données SOAP sur l'instance. Si des utilisateurs accèdent actuellement à ces données, ils sont restreints/autorisés à accéder aux données en fonction des règles ACL. Pour connaître les rôles par défaut qui ont accès aux données SOAP, reportez-vous à la section SOAP web service .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes SOAP entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Enforce strict security for inbound SOAP SOAP web service

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Instanciateurs de connexions JMS requis [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]

La `mid.property.jms.command.allowed_factory_names` propriété contrôle les instanciateurs de connexions de Service de messagerie Java (JMS) que le Serveur MID peut utiliser.

Il est destiné à quelques instanciateurs sélectionnés requis par les plugins pour l'activité ou l'action JMS. L'inclusion d'usines supplémentaires pourrait être une étape dans une chaîne d'attaque pour des vulnérabilités telles que l'insertion JDNI qui reposent sur les capacités qu'un attaquant peut exploiter dans les usines autorisées. Pour éviter toute possibilité de vulnérabilité exploitée, n'incluez pas les usines au-delà des valeurs par défaut nécessaires.

Pour remédier à ce risque de sécurité, passez en revue la liste des noms fournie à la propriété MID, `mid.property.jms.command.allowed_factory_names`. Assurez-vous que tous les noms d'instanciateurs Java supplémentaires au-delà de la valeur par défaut connectionFactory, queueConnectionFactory et topicConnectionFactory sont nécessaires.

En savoir plus

Attribut	Description
Nom de la configuration	`mid.property.jms.command.allowed_factory_names`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Valeur recommandée	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,1 • Score CVSS : moyen • Détails du risque de sécurité : Si le module d'extension Serveur MID (*com.glideapp.agent*) est actif, passez en revue la liste des noms fournie à la propriété *mid.property.jms.command.allowed_factory_names*MID. Assurez-vous que tous les noms d'instanciateurs supplémentaires au-delà de la valeur par défaut connectionFactory, queueConnectionFactory et topicConnectionFactory sont nécessaires.
Dépendances et prérequis	Aucun

Restreindre le développement d'application global par rôle [nouveau dans Security Center 2.0]

Utilisez la *sn_g_app_creator.allow_global* propriété pour contrôler quels utilisateurs peuvent créer des applications dans le champ d'application global à l'aide du Créateur d'applications guidée.

Si *sn_g_app_creator.allow_global* est défini sur la valeur recommandée faux, les *sn_g_app_creator.global* utilisateurs ont besoin du rôle pour créer des applications dans le champ d'application global. Inversement, si la valeur non sécurisée est true, tout utilisateur ayant le rôle de base sn_g_app_creator.app_creator peut créer des applications globales. Les applications globales ne disposent pas d'une protection du champ d'application, ce qui permet aux développeurs d'accéder à des fonctionnalités et des fonctions étendues au-delà des champs d'application spécifiques. Restreindre le développement d'applications globales aux utilisateurs ayant le rôle supplémentaire adhère au principe du moindre privilège.

Remarque :
Cette propriété n'est pas préconfigurée dans votre instance. Vous devez créer et configurer manuellement cette propriété en fonction des besoins de votre organisation.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_g_app_creator.allow_global*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	Faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,3 • Score CVSS : faible • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur la valeur recommandée, n'importe quel utilisateur doté du rôle s peut créer des applications globales`n_g_app_creator.app_creator` , ce qui n'adhère pas au principe du moindre privilège.
Dépendances et prérequis	Aucun
Impact fonctionnel	Amélioration de l'API (/api/now/templates) pour valider l'ACL et la propriété Créer une application globale.

Examiner les conditions de contrôle d'accès au rôle explicite superflu [Supprimé dans Centre de sécurité 1.5]

Le module d'extension Explicit Roles est recommandé pour exiger que tous les utilisateurs disposent soit du rôle snc_internal pour accéder aux ressources internes, soit du rôle snc_external pour accéder aux ressources externes.

Après l'installation de ce module d'extension, tous les utilisateurs existants se voient affecter le rôle snc_internal et les listes de contrôle d'accès (ACL) existantes sont remplies avec les conditions de rôle. En raison de la logique d'automatisation ou de l'intervention d'un administrateur d'instance, les rôles snc_internal ou snc_external peuvent être ajoutés de manière incorrecte à une ACL qui contient déjà une exigence de rôle plus stricte. Étant donné que l'évaluation du rôle ACL s'appliquera à tout utilisateur contenant un rôle mappé à une ACL, l'ajout de snc_internal ou de snc_external peut être trop large pour l'objectif prévu d'une ACL. Cela peut entraîner une fuite de données si un utilisateur ayant peu de privilèges se voit accorder l'accès via l'ACL.

Par exemple, il serait inutile que les rôles snc_internal et administrateur soient mappés à la même ACL dans une table. L'ACL est censée accorder l'accès aux administrateurs, auquel cas le rôle snc_internal est une erreur. L'ACL est également destinée à accorder l'accès à tous les utilisateurs snc_internal, ce qui rend le rôle administrateur inutile. Lorsque le module d'extension Explicit Roles est installé, examinez les ACL qui contiennent une condition de rôle pour snc_internal ou snc_external tout en contenant une condition pour un autre rôle. Si les rôles peuvent fonctionner pour un cas d'utilisation spécifique, le résultat doit être révisé périodiquement.

Important :
Ce paramètre de sécurisation renforcée sera supprimé dans la prochaine version du correctif du magasin Security Center v1.5 et dans les versions futures. Une suite d'analyse d'instance appelée « Explicit Roles ACL Config Check Suite » est disponible dans la version Washington. Nous vous recommandons de passer en revue les conclusions de cette nouvelle analyse d'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir l'utilisateur invité pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Configurez cette propriété pour contrôler le niveau d'accès des demandes SOAP non authentifiées.

Cette propriété contrôle le niveau d'accès des demandes SOAP non authentifiées. S'il n'est pas défini sur la valeur recommandée de *soap.guest*, ou s'il est défini sur un utilisateur avec des privilèges limités, les demandes SOAP s'exécuteront au nom de l'utilisateur. Si cette propriété est vide, elle active l'accès non authentifié aux opérations de niveau administrateur ou maintenance, ce qui annule tous les contrôles de sécurité au sein de l'instance.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.soap.guest_user*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	soap.guest
Valeur par défaut	soap.guest
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur vide permet un accès non authentifié aux opérations de niveau administrateur ou maintenance.
Dépendances et prérequis	Aucun

Désactiver l'accès public aux favoris [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Utilisez les *glide.ui.magellan.favorites.allow_public* pour spécifier si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.

L'accès public aux favoris est conforme lorsque *glide.ui.magellan.favorites.allow_public* cette option est définie sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.magellan.favorites.allow_public*
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Contrôlez si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.
Type	vrai/faux
Valeur recommandée	`false`
Dépendances de Sécurité	Défini sur `glide.ui.magellan.favorites.allow_public`**faux**.
Impact fonctionnel	(Moyen) L'activation de cette propriété agit comme une couche de protection contre les utilisateurs non autorisés.
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé à des données sensibles.
Références	Configure favorites option

Activer le module d'extension du contrôle d'accès SNC [Mis à jour dans Centre de sécurité 1.3]

Activez le module d'extension SNC Access Control (com.snc.snc_access_control) pour contrôler l'accès à vos instances par Service client et assistance le personnel.

Empêchez ServiceNow le personnel du service clientèle et de l'assistance d'accéder aux instances sans votre autorisation expresse en activant le module d'extension SNC Access Control (com.snc.snc_access_control). Bien que tous les accès à votre instance soient audités, vous préférez peut-être contrôler cet accès. Cette méthode d'accès est entièrement auditable et suivie.

Remarque :
D'autres membres du personnel d'exploitation autorisés ServiceNow , dans leur capacité à prendre en charge et à gérer le produit, sont tenus d'effectuer des actions administratives sur l'infrastructure sous-jacente. L'activation de ce module d'extension peut affecter les niveaux de service d'assistance et le SLA de disponibilité. La disponibilité du SLA est ensuite mesurée à partir du moment où le personnel de support est autorisé à accéder à votre instance.

Activez le module d'extension SNC Access Control (com.snc.snc_access_control) pour restreindre l'accès à votre instance sans votre autorisation expresse. Pour en savoir plus sur cette fonctionnalité, reportez-vous à la section Contrôle d'accès ServiceNow. Pour plus d'informations sur l'activation, consultez Activer ServiceNow le contrôle d'accès

En savoir plus

Attribut	Description
Nom du module d'extension	`com.snc.snc_access_control`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Contrôle d'accès
Objectif	Interdit Service client et assistance aux employés d'accéder à l'instance
Valeur recommandée	Actif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	Aucun. Il s'agit d'un module d'extension, pas d'une propriété Glide, il n'y a donc pas de valeur par défaut. Le module d'extension n'est pas installé par défaut.
Rôle requis	L'administrateur client ne peut pas activer ce module d'extension. Elle doit être explicitement demandée, car elle nécessite des privilèges élevés pour activer le module d'extension.
Cote de risque de sécurité	3.3
Impact fonctionnel	Si ce module d'extension est inactif, tous les Service client et assistance employés peuvent accéder à l'instance du client. L'activation du module d'extension permet au client de restreindre l'accès aux seuls employés autorisés Service client et assistance .
Risque de sécurité	(Élevé) Exposition inutile de l'accès à l'instance à un groupe plus large de personnes.
Références	Contrôle d'accès ServiceNow

Étapes de configuration

1. Pour demander le module d'extension, suivez les étapes de la section Activer ServiceNow le contrôle d'accès. Les clients doivent demander le module d'extension SNC Access Control (com.snc.snc_access_control) auprès de HI.
2. Pour activer le contrôle de l'accès SNC, suivez les étapes de la section Configurer ServiceNow le contrôle d'accès. Configurez un enregistrement de contrôle d'accès pour spécifier un ou Service client et assistance plusieurs employés qui ont l'autorisation de se connecter dans votre instance.

Utiliser la classification de documents pour limiter les documents accessibles au public [nouveau dans Security Center 7.0]

Contrôlez l'accès public aux documents liés en permanence à l'aide de propriétés système.

Remarque :
Ce paramètre de durcissement ne fait pas partie de la base de référence de durcissement. Il n'apparaît pas dans les pages de sécurisation renforcée du Centre de sécurité et affecte votre score de sécurisation renforcée.

Par défaut, le module d'extension Gestion des documents inclut les classifications suivantes :

- **public**
- **restreint**
- **Confidentiel**
- **aucune** (aucune classification fournie)

Utilisez les `com.snc.documents.permalink.allowed_classifications` pour créer une liste de classifications de documents. Les documents sous ces classifications (et les documents sans classification) sont accessibles au public à tous les utilisateurs non authentifiés avec un lien approprié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez cette propriété pour contrôler l'accès public aux permaliens de document. Auparavant, ces liens étaient accessibles publiquement à toute personne disposant du lien. La valeur de cette propriété dépend de vos besoins spécifiques. Vous pouvez avoir d'autres catégories de documents personnalisés qui doivent être ajoutées à cette propriété pour permettre l'accès public.

Définissez la valeur de la `com.snc.documents.permalink.allowed_classifications` propriété sur une liste de classifications de documents séparées par des virgules. Les documents avec ces classifications sont publiquement accessibles aux utilisateurs non authentifiés.

Si cette propriété ne figure pas dans la table Propriétés système [sys_properties], la liste est vide par défaut. Dans ce cas, seuls les documents sans classification sont publiquement accessibles par les utilisateurs non authentifiés. La valeur par défaut de cette propriété est **public**, ce qui signifie que seuls les documents classifiés comme **publics** ou les documents sans classification sont accessibles aux utilisateurs non authentifiés.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.documents.permalink.allowed_classifications`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Liste de chaînes
Valeur recommandée	publique
Valeur par défaut	publique
Valeur de secours	<vide>
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Si une catégorie de documents contenant des documents qui ne devraient pas être accessibles au public est ajoutée à cette propriété, elle peut exposer des informations sensibles aux utilisateurs non authentifiés.
Impact fonctionnel	Si une catégorie de documents contenant des documents qui devraient être accessibles au public n'est pas ajoutée à cette propriété, l'accès à ces documents est impossible.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Valider les ACL de requête sur les fonctions de base de données Glide [nouveau dans Security Center 7.0]

Contrôlez si les ACL de requête sont appliquées aux fonctions de base de données Glide à l'aide de propriétés système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque la *glide.db.encoded_query.check_function_field_query_acls* propriété système est définie sur **true**, les ACL de requête (query_range et query_match) sont validées par défaut sur ces fonctions de base de données Glide :

- Glidefonction :position
- glidefunction :sous-chaîne
- glidefonction :concaténé
- glissementfonction :fusion
- glidefonction :longueur

Pour valider ces ACL de requête sur des fonctions supplémentaires, ajoutez ces fonctions à la *glide.db.encoded_query.force_query_range_on_functions* propriété système.

Définissez la *glide.db.encoded_query.check_function_field_query_acls* propriété système sur **vrai** ou confirmez que la propriété ne figure pas dans la liste Propriétés système [sys_properties].

En savoir plus

Attribut	Description
Nom de la configuration	• *glide.db.encoded_query.check_function_field_query_acls* • *glide.db.encoded_query.force_query_range_on_functions*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	• Booléen • Liste de chaînes
Valeur recommandée	• vrai • glidefunction :position, glidefunction :sous-chaîne, glidefunction :concat, glidefunction :coalesce, glidefunction :length
Valeur par défaut	• vrai • glidefunction :position, glidefunction :sous-chaîne, glidefunction :concat, glidefunction :coalesce, glidefunction :length
Valeur de secours	• vrai • glidefunction :position, glidefunction :sous-chaîne, glidefunction :concat, glidefunction :coalesce, glidefunction :length
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Si la *glide.db.encoded_query.check_function_field_query_acls* propriété système existe et n'est pas définie sur la valeur **vrai**, un utilisateur connecté peut être en mesure de déduire les données aveuglément, ce qui entraîne la divulgation d'informations sensibles.
Impact fonctionnel	Les utilisateurs peuvent s'attendre à voir des valeurs des champs de fonction, mais ils sont bloqués en raison des ACL appliquées aux champs de fonction.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

API et service web

La catégorie API et Service Web garantit que les applications disposent d'une authentification, d'une autorisation et d'une gestion des sessions appropriées, valident toutes les entrées qui traversent une limite de confiance et incluent des contrôles de sécurité pour tous les types d'API.

Des contrôles spécifiques dans cette catégorie traitent la validation de l'entrée par type de service, tels que la validation de schéma XDS pour les services Web SOAP ou la protection contre le déni de service pour les API GraphQL.

Valider le type de contenu SOAP [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour activer la *glide.soap.require_content_type_xml* validation d'un type de contenu comme texte/xml et protéger contre les demandes SOAP invalides.

- Lorsque la valeur est définie sur **vrai**, l'émetteur ServiceNow AI Platform valide le type de contenu comme text/xml et protège contre les demandes SOAP invalides.
- Si la valeur est définie sur **faux**, toute valeur de type de contenu est autorisée.

> **⚠ Avertissement :**
> Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.soap.require_content_type_xml*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Protéger contre les demandes SOAP invalides
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette correction active la validation du type de contenu SOAP pour toutes les demandes SOAP entrantes. • Si vous utilisez un type de contenu autre que texte/xml pour les demandes entrantes, cela peut entraîner l'échec potentiel des transactions SOAP. • Si vous n'utilisez pas le type MIME correct, cela peut perturber les intégrations tierces.
Risque de sécurité	(Modéré) Lors de l'acceptation de demandes SOAP entrantes, la validation appropriée est effectuée pour s'assurer que le type de contenu approprié est défini dans le cadre de la demande. Il restreint les réponses SOAP non valides qui peuvent être considérées comme un risque de sécurité.
Référence	Types de contenu

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes PDF [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.pdf` demandes PDF entrantes doivent nécessiter une authentification de base.

Assurez-vous que la propriété `glide.basicauth.required.pdf` existe dans la table sys_properties et qu'elle est définie sur vrai.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.pdf`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes PDF.
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données PDF sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez Jeux d'importation de services web .
Risque de sécurité	(Élevé) Si l'autorisation appropriée n'est pas configurée sur les demandes PDF entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger l'authentification sur le processeur HTTP de Gestion des événements [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et supprimé dans la version 2.0]

Découvrez comment établir une authentification de base sécurisée pour les demandes Amazon Simple Notification Service (SNS) entrantes lorsque le module d'extension Gestion des événements (`com.glideapp.itom.snac`) est activé.

Si la `glide.basicauth.required.evtmgmthttpprocessor` propriété n'est pas définie sur la valeur conseillée **vrai** et que le module d'extension Gestion des événements (`com.glideapp.itom.snac`) est actif, l'authentification de base n'est pas requise pour toutes les demandes Amazon Simple Notification Service (SNS) entrantes. Cela peut entraîner un accès non authentifié aux données d'instance.

Pour remédier à ce risque de sécurité, assurez-vous que est `glide.basicauth.required.evtmgmthttpprocessor` défini sur**vrai** et que `com.glideapp.itom.snac` actif.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.evtmgmthttpprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	vrai
Catégorie	API et service web
Risque de sécurité	• Score de gravité : 7 • Score CVSS : élevé • Détails du risque de sécurité : le fait de ne pas définir`glide.basicauth.required.evtmgmthttpprocessor` la valeur recommandée vrai et de ne pas activer le module d'extension entraîne l'absence d'activation de l'authentification `com.glideapp.itom.snac` de base pour les demandes SNS entrantes. Cela peut entraîner un accès non authentifié aux données d'instance.
Dépendances et prérequis	Aucun
Références	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Access control
Impact fonctionnel	Si `glide.basicauth.required.evtmgmthttpprocessor` n'est pas défini sur la valeur recommandée Vrai et si le module d'extension Gestion des événements (com.glideapp.itom.snac) est actif, l'authentification de base n'est pas requise pour toutes les demandes SNS entrantes des services web Amazon. Cela peut entraîner un accès non authentifié aux données d'instance.

Exiger une autorisation pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.soap` demandes SOAP entrantes doivent obtenir une autorisation de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.soapglide.soap.require_ws_securi`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'autorisation des demandes SOAP.
Valeur recommandée	vrai
Cote de risque de sécurité	8.1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données SOAP sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui doit avoir accès à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour plus d'informations, consultez les informations d'identification d'authentification du service Web SOAP et du serveur MID et les demandes SOAP .SOAP web service
Risque de sécurité	(Moyen) Sans l'autorisation appropriée configurée sur les demandes SOAP de la source de données, un utilisateur non autorisé peut accéder au contenu/aux données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes de déchargement [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent nécessiter une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.unl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes de déchargement.
Valeur recommandée	vrai
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données non téléchargées sur l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de déchargement de source de données, un utilisateur non autorisé peut accéder à du contenu/ des données sensibles sur l'instance cible. Assurez-vous que existe dans la sys_properties_table et qu'il `glide.basicauth.required.unl` est défini sur vrai.
Références	Authentification

Exiger une autorisation pour les demandes CSV [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.csv` demandes CSV entrantes (valeurs séparées par des virgules) doivent nécessiter une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.csv`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux requêtes CSV.
Valeur recommandée	vrai
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données CSV sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, voir Récupération des données d'un fichier au format CSV .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes CSV entrantes, un utilisateur non autorisé peut accéder à du contenu et à des données sensibles sur l'instance cible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Assurez-vous qu'il existe dans la table sys_properties et qu'il `glide.basicauth.required.csv` est défini sur vrai.
Références	Sécurité des services Web

Exiger une autorisation pour les demandes Excel [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.excel` demandes Excel entrantes doivent nécessiter une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.excel`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes Excel.
Valeur recommandée	vrai
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données Excel sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes Excel entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes d'importation [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.importprocessor` demandes d'importation entrantes doivent nécessiter une authentification de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.importprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes d'importation.
Valeur recommandée	vrai
Cote de risque de sécurité	5.3
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification lors de l'importation de sources de données dans les tables/pages de l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, voir Récupération des données d'un fichier au format CSV .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes d'importation de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Sécurité des services web SOAP Service web SOAP

Exiger une autorisation pour la demande JSONv2 [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.jsonv2` demandes JSONv2 entrantes doivent requiert une autorisation de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.jsonv2`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'autorisation des demandes JSONv2.
Cote de risque de sécurité	7.5
Valeur recommandée	vrai
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données JSON sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui doit avoir accès à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour plus d'informations, consultez Service web JSONv2 Service web JSONv2 .
Risque de sécurité	(Élevé) Sans l'autorisation appropriée configurée sur les demandes JSON de source de données, un utilisateur non autorisé peut accéder au contenu/aux données sensibles sur l'instance cible.
Références	Authentification Authentification de base requise pour les demandes JSONv2 entrantes

Exiger une autorisation pour la demande WSDL [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.wsdl` demandes WSDL (Web Services Description Language) entrantes doivent exiger une authentification de base.

Si `glide.basicauth.required.wsdl` n'est pas défini sur la valeur recommandée vrai, alors , cela désactive l'authentification de base pour les demandes WSDL. WSDL est un protocole utilisé pour décrire les services Web tels que les schémas de table d'instance, et n'est pas un mécanisme de partage des données au sein de tables. Définir cette propriété sur vrai permet la divulgation des schémas de table aux utilisateurs non authentifiés.

Remarque :
Si vous choisissez de ne pas exiger l'authentification de base pour les demandes WSDL entrantes, vous devez modifier les règles de contrôle d'accès (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.wsdl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes WSDL.
Valeur recommandée	vrai
Cote de risque de sécurité	5.3
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données WSDL sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les services Web WSDL, un utilisateur non autorisé peut accéder à du contenu/des données WSDL sensibles sur l'instance cible.
Références	Sécurité des services Web

Exiger une autorisation pour les demandes XML [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.xml` demandes XML entrantes doivent nécessiter une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.xml`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour appliquer l'authentification de base aux demandes XML.
Cote de risque de sécurité	7.5
Valeur recommandée	vrai
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données XML sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez Étape de l'analyseur XML .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes XML entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Exiger une autorisation pour les demandes de sortie XML [Mis à jour dans Centre de sécurité 1.3]

Configurez cette propriété de manière à ce qu'une autorisation de base soit requise pour toutes les demandes XMLOutputProcessor entrantes.

Si la `glide.basicauth.required.xmloutputprocessor` propriété n'est pas définie sur la valeur conseillée **true**, l'autorisation de base n'est pas requise pour les demandes XMLOutputProcessor entrantes, pouvant entraîner une divulgation d'informations non authentifiées de l'instance.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.xmloutputprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	API et service web
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails **du risque** de sécurité : ne pas définir la propriété sur la valeur recommandée vrai peut entraîner une fuite d'informations sensibles de l'instance.
Dépendances et prérequis	Aucun

Exiger une autorisation pour les demandes XSD [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les *glide.basicauth.required.xsd* demandes XSD (définition de schéma XML) entrantes doivent nécessiter une authentification de base.

Assurez-vous que la propriété *glide.basicauth.required.xsd* existe dans la table sys_properties et qu'elle est définie sur vrai.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	glide.basicauth.required.xsd*glide.basicauth.required.xsd*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes XSD.
Valeur recommandée	vrai
Cote de risque de sécurité	5.3
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données XSD sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, voir Sessions non interactives .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes XSD entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Exiger une autorisation pour les demandes de script [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.scriptedprocessor` demandes de script entrantes doivent nécessiter une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.scriptedprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes de script.
Valeur recommandée	vrai
Cote de risque de sécurité	7.2
Impact fonctionnel	Cette correction renforce l'authentification sous la forme d'une autorisation de base. • Il effectue cette authentification lors du traitement des demandes de script sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de script entrantes, un utilisateur non autorisé accède au contenu/aux données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes SCHEMA [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour exiger une `glide.basicauth.required.schema` autorisation de base pour toutes les demandes de processeur de schéma de table entrante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le processeur Schebma de table entrante gère les demandes de schéma entrantes pour la plateforme.

Définissez `glide.basicauth.required.schema` la valeur recommandée sur **vrai** pour exiger l'autorisation de base pour toutes les demandes du processeur de schéma de table entrante. Définissez la valeur sur **faux** pour ne pas exiger d'autorisation de base pour toutes les demandes du processeur de schéma de table entrante.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.schema`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour exiger une autorisation de base pour toutes les demandes du processeur de schéma de table entrante.
Valeur recommandée	True (valeur par défaut).
Type de configuration	Booléen
Risque de sécurité	(Modéré) Omettre l'authentification à partir de ce processeur entraînera un accès non authentifié aux données d'instance.

Exiger une autorisation pour les demandes RSS [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.rss` demandes RSS entrantes doivent nécessiter une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.rss`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes RSS.
Valeur recommandée	vrai
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Il effectue cette authentification lors du traitement des demandes RSS sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, voir Générateur de flux RSS .
Risque de sécurité	(Élevé) Si l'autorisation appropriée n'est pas configurée sur les demandes RSS entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification de base RSS

Exiger une autorisation pour les demandes API [Mis à jour dans Centre de sécurité 1.3]

Utilisez cette propriété pour renforcer la `glide.basicauth.required.api` sécurité de l'autorisation de base pour les demandes REST entrantes.

Définissez la `glide.basicauth.required.api` propriété sur **vrai** pour demander une autorisation pour toutes les demandes REST. Définissez la propriété sur **faux** pour contourner l'autorisation pour toutes les demandes REST.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.api`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Autorisation de base pour les demandes REST entrantes.
Valeur recommandée	True (par défaut)
Type de configuration	Chaîne
Risque de sécurité	(Élevé) Si « glide.basicauth.required.api » n'est pas défini sur la valeur recommandée « vrai », cela désactive l'authentification de base sur la demande d'API et entraîne un accès non authentifié aux données d'instance.
Cote de risque de sécurité	8.6

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture, conception et modélisation des menaces

Ce contrôle étendu traite les considérations de conception de haut niveau et les éléments clés pour implémenter une application sécurisée. Cela couvre les locataires de la disponibilité, l'intégrité du traitement de la confidentialité, la non-répudiation et la confidentialité. De plus, des éléments d'un cycle de vie de développement logiciel sécurisé sont inclus.

Authentification basée sur certificat non mise en application [Nouveau dans Security Center 1.3]

La *glide.authenticate.mutual.enabled* propriété active l'authentification basée sur certificat, un type d'authentification réciproque pour les connexions REST entrantes aux API REST et SOAP dans le ServiceNow AI Platform.

L'authentification réciproque établit la confiance entre le serveur et le client en échangeant des certificats SSL (secure socket layer) pour valider le certificat auprès d'une autorité de certification approuvée. Cela permet de vérifier qu'une ServiceNow AI Platform source de confiance se connecte au . Si cette instance n'est pas définie sur la valeur recommandée true, une instance peut être vulnérable aux attaques de l'intercepteur (MitM).

Pour remédier à cette menace de sécurité, activez l'authentification réciproque pour les services Web entrants. Si c'est la première fois que vous installez le module d'extension d'authentification basée sur certificat (*com.glide.auth.mutual)* pour le ServiceNow AI Platform, suivez les Configurer l'authentification basée sur certificat instructions. En outre, assurez-vous que la *glide.authenticate.mutual.enabled* propriété est définie sur vrai pour activer le module d'extension.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.authenticate.mutual.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée vrai, l'authentification basée sur certificat ne valide pas les certificats auprès d'une autorité de certification approuvée. Cela augmente les chances qu'un acteur malveillant attaque une instance à l'aide d'attaques MitM.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Authentification basée sur certificat • Configurer l'authentification réciproque

Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Utilisez la propriété pour empêcher un utilisateur d'emprunter l'identité *sn_hr_core.impersonateCheck* d'un autre utilisateur et d'accéder à ses informations RH.

Un paramètre sécurisé empêche un administrateur de voir les informations RH d'un autre utilisateur lorsqu'il utilise l'emprunt d'identité. Un paramètre non sécurisé pour cette propriété permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder aux données RH telles que les résultats d'enquête ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée. En raison de la nature de ce type de données, telles que les informations qui ne devraient être disponibles que pour l'utilisateur lui-même, comme les e-mails, cela n'est pas recommandé. La valeur *sn_hr_core.impersonateCheck* vrai permet uniquement d'accéder aux informations RH lorsque l'utilisateur n'emprunte pas l'identité d'une autre personne.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_hr_core.impersonateCheck*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	Faux
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : un paramètre non sécurisé pour cette propriété permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder aux données RH telles que les résultats d'enquête ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, elle empêche un administrateur de voir les informations RH d'un autre utilisateur lors de l'emprunt d'identité. Lorsqu'elle est définie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	sur faux, elle permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder aux données RH telles que les résultats d'enquête ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée. En raison de la nature de ce type de données, telles que les informations qui ne doivent être disponibles que pour l'utilisateur lui-même comme un e-mail, cela n'est pas recommandé. Définir sn_hr_core.impersonateCheck sur vrai permet uniquement d'accéder aux informations RH lorsque l'utilisateur n'emprunte pas l'identité d'une autre personne.

Désactiver la connexion locale pour les utilisateurs avec l'authentification unique (SSO) activée

Mettez à jour les enregistrements des utilisateurs pour désactiver la connexion locale pour les utilisateurs avec l'authentification unique (SSO) activée.

Les utilisateurs configurés pour utiliser l'authentification SSO peuvent accéder à l'instance ou à certaines parties de l'instance avec des informations d'identification locales stockées dans le champ **user_password** de leur enregistrement d'utilisateur [sys_user]. Cet accès s'applique à la fois à l'accès interactif et non interactif pour les utilisateurs qui ne sont pas bloqués. Empêchez les utilisateurs configurés pour SSO d'utiliser des informations d'identification locales afin de réduire les risques de vol d'informations d'identification de connexion locales valides et d'utilisation par des utilisateurs malveillants.

Consultez l'article de la base de connaissances Now Support KB1649420 pour obtenir des instructions sur l'identification et le traitement des comptes avec une connexion locale toujours activée sur une instance avec SSO activé.

En savoir plus

Attribut	Description
Risque de sécurité	Lorsque l'authentification SSO est activée pour un utilisateur, il est recommandé d'empêcher cet utilisateur de se connecter localement. Cela réduit le risque que les identifiants de connexion locaux valides soient volés et utilisés pour se connecter par un utilisateur malveillant.
Score du système de notation des vulnérabilités courantes (CVSS)	4.2
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	Les utilisateurs configurés SSO peuvent se connecter avec des informations d'identification locales.
Dépendances et prérequis	L'authentification unique doit être activée (propriété système **glide.authenticate.multisso.enabled** définie sur **vrai**).
Type de données	N/A
Valeur de système de base	N/A
Valeur de secours	N/A
Valeur recommandée	N/A

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver les rapports publiés non authentifiés [Mis à jour dans Centre de sécurité 2.0]

Désactivez cette propriété pour empêcher l'utilisateur de publier ou d'accéder aux rapports. Cette propriété désactive la fonctionnalité de rapports publiés dans la génération de rapports.

Activez la publication de rapports en définissant l'option sur *glide.report.published_reports.enabled***vrai**.

Assurez-vous que la propriété *glide.report.published_reports.enabled* Glide existe et qu'elle est définie sur la valeur faux. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.report.published_reports.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Désactive la fonctionnalité des rapports publiés dans la génération de rapports.
Type	vrai | faux
Valeur recommandée	**false**
Cote de risque de sécurité	6.5
Impact fonctionnel	L'utilisateur ne peut pas publier de rapports.
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, les utilisateurs peuvent être en mesure d'accéder aux rapports exposant des données sensibles ou de les publier. La publication d'un rapport crée une URL que tout le monde peut utiliser pour accéder au rapport, y compris les personnes qui ne sont pas des utilisateurs. Lorsque quelqu'un navigue vers l'URL, le rapport est généré avec les données actuelles de l'instance.
Références	Publier un rapport

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Renforcer les ACL de champs pour les demandes entrantes

Gérez la façon dont les requêtes entrantes sont validées sur votre instance.

Utilisez cette propriété pour vérifier comment *glide.export.query.enforce_field_acl* les requêtes entrantes sont validées sur votre instance. Si la propriété est définie sur la valeur recommandée **vrai**, les ACL de champ sont vérifiées par rapport aux requêtes entrantes, puis rejetées si l'utilisateur n'est pas autorisé. Si la propriété est définie sur **faux**, les ACL ne sont pas vérifiées par rapport aux requêtes entrantes et continuent de s'exécuter, ce qui peut entraîner la divulgation d'informations à des parties non autorisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.export.query.enforce_field_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété est définie sur **faux**, les ACL ne sont pas vérifiées par rapport aux requêtes entrantes pouvant entraîner la divulgation d'informations.
Dépendances et prérequis	Aucun

Appliquer les ACL en lecture sur les vues de rapport

Gérez la façon dont les ACL en lecture sont appliquées sur votre instance.

Utilisez la `glide.report.report_view.read_acl` propriété pour appliquer l'ACL de lecture (au niveau de la table) sur les fonctions de génération de rapports lorsqu'il n'y a pas d'ACL de vue de rapport dans la table ou le champ. Si cette propriété n'est pas définie pour **s'appliquer**, les ACL peuvent être contournées et entraîner une fuite d'informations sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.report.report_view.read_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	appliquer
Valeur par défaut	appliquer
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : ne pas définir cette propriété sur **appliquer** pourrait entraîner le contournement des ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Dépendances et prérequis	Aucun

Appliquer les ACL de requête pour les liens rapides de la base de connaissances

Appliquez des ACL de requête pour les liens rapides de la base de connaissances à l'aide d'une propriété système.

Lorsque la *com.glide.security.query_acl.enabled.knowledge_quick_links* propriété système est définie sur **true**, les ACL de requête sont appliquées pour les liens rapides de la base de connaissances. Si cette propriété est définie sur **faux**, un attaquant peut utiliser des requêtes aveugles pour énumérer et exfiltrer des données en raison du comportement par défaut de GlideRecord.addEncodedQuery.

Si la propriété n'existe pas dans la table Propriétés système [sys_properties], la valeur par **défaut sécurisée True** est utilisée. Une troisième option, **external_and_guests** applique les ACL de requête uniquement pour les utilisateurs externes et les invités.

Vérifiez que la *com.glide.security.query_acl.enabled.knowledge_quick_links* propriété système est définie sur **true**.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.security.query_acl.enabled.knowledge_quick_link*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Chaîne : utilisé comme opérateur ternaire
Valeur recommandée	vrai
Valeur par défaut	vrai
Valeur de secours	vrai
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Risque de sécurité : les ACL peuvent être contournées, ce qui divulgue les données du champ aux utilisateurs qui n'ont pas l'autorisation de les voir. Cette divulgation pourrait inclure des données sensibles selon la table exploitée.
Impact fonctionnel	Les utilisateurs ne sont pas en mesure d'effectuer des requêtes spécifiques sur les champs auxquels ils n'ont pas accès au niveau du champ.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les ACL de requête pour les sous-listes, les nombres de listes et les tables de données de widget

Appliquez les ACL de requête sur les requêtes de table de données de sous-liste, de nombre de listes et de widget à l'aide de propriétés système.

Définissez *com.glide.security.query_acl.enabled.sub_lists* la valeur **sur vrai** pour appliquer les ACL de requête sur les requêtes de sous-liste, telles que les listes groupées et les listes connexes.

Définissez *com.glide.security.query_acl.enabled.list_count* la valeur **sur vrai** pour appliquer les ACL de requête aux requêtes de comptage de listes.

Définissez *glide.security.query_acl.enabled.data_table* la valeur **sur vrai** pour appliquer les ACL de requête sur les tables de données de widget.

Si l'une de ces propriétés système est définie sur **faux**, un attaquant peut utiliser des requêtes aveugles pour énumérer et exfiltrer des données en raison du comportement par défaut de GlideRecord.addEncodedQuery. Si ces propriétés n'existent pas dans la table Propriétés système [sys_properties], la valeur par défaut sécurisée true est utilisée. Une troisième option, *external_and_guests*, applique les ACL uniquement aux utilisateurs externes et aux invités.

Assurez-vous que ces propriétés système n'apparaissent pas dans la table Propriétés système [sys_properties] ou qu'elles sont définies sur **vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	• *com.glide.security.query_acl.enabled.sub_lists* • *com.glide.security.query_acl.enabled.list_count* • *glide.security.query_acl.enabled.data_table*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	• vrai • vrai • vrai
Valeur par défaut	• vrai • vrai • vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur de secours	• vrai • vrai • vrai
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Risque de sécurité : les ACL peuvent être contournées en divulguant des données de champ à des utilisateurs qui n'ont pas l'autorisation de les voir. Cela peut inclure des données sensibles en fonction de la table exploitée.
Dépendances et prérequis	Aucun

Appliquer un choix de chaîne de requête valide [Nouveau dans Security Center 7.0]

Utilisez une propriété système pour vous assurer que toute valeur de champ de choix, lorsqu'elle est transmise via une chaîne de requête URL, est un choix actif valide lors de la création d'un enregistrement.

Lorsque la `glide.ui.query_string.enforce_valid_choice_on_create` propriété système est définie sur **vrai**, la plateforme valide que toute valeur de champ de choix transmise via une chaîne de requête URL (par exemple, à partir d'un filtre de liste) est un choix actif valide lors de la création de l'enregistrement.

Si elle n'est pas valide, la valeur est ignorée et le champ revient à sa valeur par défaut. Lorsque la propriété est **définie sur faux**, la validation est inactive et le système accepte toutes les valeurs, même non valides ou inactives. Cette acceptation peut potentiellement entraîner le stockage de données incorrectes ou inattendues sur des enregistrements.

Ensure `glide.ui.query_string.enforce_valid_choice_on_create` existe dans la table Propriétés système [sys_properties] et est défini sur **vrai**. Si la propriété n'existe pas dans la table, la valeur de secours est **faux**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.query_string.enforce_valid_choice_on_create`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Valeur de secours	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 2,2 • Score CVSS : faible • Risque pour la sécurité : définissez cette propriété sur **vrai** pour vous assurer que seuls des choix valides sont utilisés pour la création d'un nouvel enregistrement. Des choix non valides peuvent entraîner des problèmes d'intégrité des données mineurs et inattendus, où un utilisateur est en mesure de sélectionner une valeur non prévue.
Impact fonctionnel	Les instances et les workflows existants peuvent dépendre de la création de nouveaux enregistrements en fonction d'un filtre qui contient un choix non valide ou inactif. Utilisez le processus suivant pour observer ce comportement : **1.** Connectez-vous à une instance en tant qu'utilisateur administrateur. **2.** Créez un champ Chaîne dans n'importe quelle table. Par exemple, un incident avec 2 choix : **Test1** et **Test2**. **3.** Créez un filtre de liste sur la table d'incidents en sélectionnant le champ de chaîne avec la valeur définie sur **Test2**. **4.** Accédez au champ du dictionnaire et désactivez le choix **Test2**. **5.** Accédez au filtre sélectionné à l'étape 3 et sélectionnez **le bouton Nouveau** . **6.** Vérifiez la valeur du champ Type de chaîne dans l'enregistrement qui vient d'être ouvert. Lorsque la propriété est définie sur **vrai**, le champ chaîne ne doit pas avoir de valeur ou doit afficher la valeur par défaut. Lorsque la propriété est définie sur **false** (valeur par défaut), la valeur du champ de chaîne est définie sur **Test2**.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les adresses IP internes autorisées ServiceNow [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour spécifier les `glide.ip.authenticate.strict` plages IP qui peuvent établir des connexions entrantes sur une instance.

Empêchez l'exposition inutile de l'accès à l'instance à un groupe plus large de personnes à l'aide des propriétés système **glide.ip.authenticate.strict** et **glide.ip.authenticate.allow.secured** .

Lorsque la propriété système **glide.ip.authenticate.strict** est définie sur **vrai**, le personnel et les systèmes internes ServiceNow ne peuvent établir des connexions entrantes vers votre instance qu'à partir des plages IP essentielles. Cela limite ServiceNow la visibilité de l'infrastructure interne essentielle sur votre instance et empêche l'accès par un personnel plus large tel que le personnel de ServiceNow support et de vente via les réseaux de l'entreprise. La propriété système **glide.ip.authenticate.allow.secured** accorde des connexions entrantes internes ServiceNow , y compris un accès authentifié régulier et des pages de diagnostic non authentifiées.

Si la valeur n'est pas définie sur **vrai**, une plage d'adresses IP interne plus large ServiceNow définie dans la propriété **glide.ip.authenticate.allow** est utilisée pour accorder ces connexions entrantes internes ServiceNow .

Assurez-vous que la propriété système **glide.ip.authenticate.allow.secured** contient uniquement des valeurs fiables et que la propriété **glide.ip.authenticate.strict** est définie sur **vrai**.

⚠ Avertissement :
La valeur de cette propriété est un remplacement sans base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ip.authenticate.strict`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Permet aux employés de ServiceNow d'accéder à l'instance uniquement via un ensemble sécurisé de plages IP
Valeur recommandée	vrai
Cote de risque de sécurité	4.3
Impact fonctionnel	(Faible) Si cette propriété n'est pas activée, les employés de ServiceNow peuvent accéder à l'instance du client via toutes les plages IP. L'activation de la propriété restreint l'accès à un ensemble sécurisé de plages IP (VPN sécurisé, DC).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Remarque : Si vous définissez cette propriété sur `vrai`, le utilise ServiceNow AI Platform une propriété plus restrictive `glide.ip.authenticate.allow.secured` que la propriété de restriction IP de surveillance des performances (`glide.ip.authenticate.allow.secured`) pour un ensemble de plages IP pouvant accéder à l'instance.
Risque de sécurité	(Faible) Exposition inutile de l'accès à l'instance à un groupe plus large de personnes.
Référence	Authentification basée sur la plage IP

Remarque : Une règle refuser tout doit être ajoutée au contrôle d'accès IP pour restreindre l'accès à partir de toute adresse IP non ajoutée au contrôle d'accès IP. Toutes les adresses IP autorisées requises doivent ensuite être ajoutées au contrôle d'accès IP.

Désactiver le comportement JQuery hérité [Mis à jour dans Security Center 1.3]

Ceci `glide.jquery.legacy` est utilisé pour empêcher l'utilisation d'anciennes versions jQuery prédéfinies qui introduiront des vulnérabilités non corrigées dans la bibliothèque.

Définissez `glide.jquery.legacy` la valeur recommandée sur **faux** pour empêcher l'utilisation d'anciennes versions jQuery prédéfinies qui introduisent des vulnérabilités non corrigées dans la bibliothèque. Définissez la valeur sur **vrai** pour autoriser les versions jQuery prédéfinies.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.jquery.legacy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Pour prévenir les risques de sécurité potentiels découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque jQuery obsolètes.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Empêchez l'utilisation d'anciennes versions jQuery prédéfinies qui introduisent des vulnérabilités non corrigées dans la bibliothèque. La propriété système est une sécurité au cas où des organisations dépendent des versions non corrigées d'AngularJS pour exécuter leurs implémentations personnalisées.
Cote de risque de sécurité	7.1

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]

La `glide.record.legacy_cross_scope_access_policy_in_script` propriété désactive la séparation des champs d'application permettant aux applications incluses dans le périmètre d'accéder aux interfaces de script globales. Il a été créé en tant que correctif pour l'accès multi-champs d'application de GlideRecord.

GlideRecord a fourni un accès de création/mise à jour entre périmètres à des tables qui n'ont pas été configurées avec ce niveau d'accès. Afin d'éviter que les applications des clients ne soient interrompues lorsque ce comportement d'accès inclus dans le périmètre est corrigé, la propriété `glide.record.legacy_cross_scope_access_policy_in_script` a été créée. Si la valeur est vrai, l'accès entre périmètres revient au comportement hérité (non sécurisé). Cette propriété désactive la séparation des périmètres, ce qui permet aux applications incluses dans le périmètre d'accéder aux interfaces de script globales.

Il est préférable de mettre en place des restrictions de clôture de portée. La définition du champ d'application garantit que les applications ne peuvent accéder aux ressources qu'avec un accès explicite ou dans leur champ d'application, conformément au principe du moindre privilège. La désactivation de cette fonctionnalité peut entraîner des impacts sur la confidentialité, la disponibilité et l'intégrité.

Définissez la propriété `glide.record.legacy_cross_scope_access_policy_in_script` Glide sur faux. Lorsqu'elle n'est pas présente dans la table sys_properties, la valeur par défaut est vrai.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.record.legacy_cross_scope_access_policy_in_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai (lorsque la propriété n'existe pas dans la table sys_properties.)
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5 • Score CVSS : moyen • Détails du risque de sécurité : la définition du champ d'application garantit que les applications ne peuvent accéder aux ressources qu'avec un accès explicite ou dans leur champ d'application, conformément au principe des privilèges minimum. La désactivation de cette fonctionnalité peut entraîner des impacts sur la confidentialité, la disponibilité et l'intégrité.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le comportement AngularJS hérité [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour vous protéger contre les `glide.angular.legacy` risques de sécurité potentiels découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque AngularJS obsolètes.

Définissez `glide.angular.legacy` la valeur recommandée sur **faux** pour empêcher l'utilisation d'anciennes versions AngularJS prédéfinies. Définissez la propriété sur **vrai** pour utiliser les anciennes versions AngularJS prédéfinies.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.angular.legacy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	La propriété système est une sécurité au cas où des organisations dépendent des versions non corrigées d'AngularJS pour exécuter leurs implémentations personnalisées.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) L'utilisation d'anciennes versions d'AngularJS peut potentiellement entraîner des risques de sécurité découlant d'attaques sur les vulnérabilités détectées dans les versions de bibliothèque AngularJS obsolètes.
Cote de risque de sécurité	7.1

Exiger une autorisation pour l'API REST du courtier en données [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour exiger une `glide.basicauth.required.databrokerrestapiprocessor` autorisation de base pour toutes les demandes API REST du courtier de données.

Si cette propriété est définie sur **vrai**, l'autorisation est appliquée. Si elle est définie sur **faux**, aucune autorisation n'est utilisée, ce qui pourrait entraîner la fuite d'informations sensibles de votre instance.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.databrokerrestapiprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 8,6 • Score CVSS : élevé • Détails du risque de sécurité : si la propriété est définie sur **faux**, l'authentification API n'est pas appliquée, ce qui permet à un acteur malveillant d'accéder aux données sensibles.
Dépendances et prérequis	Aucun

Fonctionnalité de liaison restreinte en cas d'autorisation du titulaire [nouveau dans le centre de sécurité 7.0]

Utilisez une propriété système et une liaison restreinte pour vous assurer qu'un jeton d'accès généré à l'aide de cette entité ne peut pas être utilisé pour les appels d'interface utilisateur.

Utilisez la propriété système et activez la `glide.oauth.enforce_restricted_binding_for_ui` liaison restreinte pour une entité OAuth afin d'empêcher l'utilisation des jetons d'accès générés par cette entité pour des appels d'interface utilisateur (par exemple, `incident_list.do`).

Lorsque la liaison restreinte est désactivée, le jeton d'accès généré peut être utilisé pour les appels d'interface utilisateur, quelle que soit la valeur de la propriété système.

Assurez-vous que `glide.oauth.enforce_restricted_binding_for_ui` est défini sur **vrai** et que **l'option Appliquer les restrictions de jeton** est définie sur **vrai** dans toutes les entrées d'entité OAuth. Pour plus d'informations sur les entrées d'entité OAuth, reportez-vous à la section Entrant OAuth.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.oauth.enforce_restricted_binding_for_ui`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Valeur de secours	Faux
Catégorie	Architecture, conception et modélisation des menaces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 5,0 • Score CVSS : moyen • Détails du risque de sécurité : lorsque la propriété système n'est pas définie sur **vrai** ou que la `glide.oauth.enforce_restricted_binding_for_ui` liaison restreinte est désactivée, un utilisateur disposant du jeton d'accès permettant d'accéder à une API (par exemple, une API mobile) peut obtenir une session émise et l'utiliser pour accéder à d'autres ressources restreintes sur l'instance (par exemple, incident_list.do).
Dépendances et prérequis	Aucun

Refuser par défaut en cas d'ACL vides [Mis à jour dans Centre de sécurité 1.3]

Utilisez la `glide.sm.default_mode` propriété pour contrôler le comportement par défaut du gestionnaire de sécurité lorsqu'il détecte que des règles de liste de contrôle d'accès (ACL) existantes font partie des règles ACL d'une table à caractère générique.

Empêchez le gestionnaire de sécurité hérité de votre instance d'autoriser l'accès aux ressources lorsqu'aucune ACL n'est définie pour cette ressource, ou s'il n'existe que des ACL au niveau de la table de caractères génériques (par exemple, incident.*). Lorsque l'accès est autorisé par défaut, tout ce qui n'a pas d'ACL explicites définies est susceptible d'être manipulé.

Définissez la valeur de la propriété système **glide.sm.default_mode** sur **refuser** pour interdire l'accès lorsqu'il n'y a pas de règles ACL définies ou qu'il n'y a que des ACL au niveau de la table de caractères génériques.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sm.default_mode`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	La meilleure pratique de sécurité serait de restreindre l'accès aux tables par un utilisateur non autorisé. • Si aucune règle ACL n'est en place pour les tables, cette propriété garantit qu'au moins les ACL génériques sont validées pour toute opération CRUD effectuée sur la table/le champ. • Ces règles restreignent les opérations de lecture, d'écriture, de création et de suppression sur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	toutes les tables, sauf si l'utilisateur a le rôle administrateur ou répond aux exigences d'une autre règle ACL de table.
Valeur recommandée	refuser
Impact fonctionnel	Si vous définissez cette propriété sur **Autoriser**, les règles ACL de la table à caractère générique autorisent les opérations CRUD sur toutes les tables, sauf s'il existe des règles ACL de table spécifiques en place pour restreindre de telles opérations. **Remarque :** Ce module d'extension n'est pas destiné aux instances existantes, car il peut modifier l'accès de sécurité aux tables qui sont déjà utilisées dans un environnement de production.
Risque de sécurité	6.3
Références	Propriété de refus par défaut

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Définir le nettoyage automatique des jetons pour les informations d'identification de jeton [nouveau dans Security Center 2.0]

Utilisez la propriété pour vous assurer que les `com.snc.platform.security.token.auth.cleanup` clés API et les secrets HMAC expirés sont supprimés, limitant ainsi le potentiel de réutilisation des jetons.

Si la `com.snc.platform.security.token.auth.cleanup` propriété est définie sur la valeur non sécurisée faux, les clés API et les secrets HMAC expirés ne sont pas supprimés, ce qui crée un potentiel de réutilisation des jetons. Si un jeton a expiré en raison d'une fuite ou d'une compromission, sa réutilisation peut exposer l'instance à toute personne possédant le jeton ayant fait l'objet de la fuite.

Les jetons expirés sont conservés pendant le nombre de jours défini par `com.snc.platform.security.token.auth.days.expired.hmac_secret.is.kept` et `com.snc.platform.security.token.auth.days.expired.api_key.is.kept`. Les valeurs valides pour ces paramètres sont des nombres entiers supérieurs ou égaux à 0. Une valeur de 0 entraîne la suppression des jetons expirés le même jour, tandis qu'un nombre de jours plus élevé augmente la période d'exposition. Une valeur par défaut de 7 jours ou moins est recommandée.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.platform.security.token.auth.cleanup`, `com.snc.platform.security.token.auth.days.expired.hmac_se`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	Les valeurs recommandées sont vrai et tout nombre entier inférieur ou égal à 7.
Valeur par défaut	7
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5,1 • Score CVSS : moyen • Détails du risque de sécurité : ne pas configurer cette propriété sur la valeur recommandée vrai peut empêcher la suppression des clés API expirées et des secrets HMAC, ce qui augmente la probabilité de réutilisation des jetons.
Dépendances et prérequis	Aucun

Authentification

La catégorie authentification couvre les principaux éléments de l'authentification moderne pour confirmer qu'une entité et ses affirmations sont authentiques et correctes, résistantes à l'usurpation d'identité et empêchent l'interception des mots de passe.

La norme ASVS s'appuie sur la spécification NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) pour cette section.

L'authentification comprend la politique, les contrôles et le stockage des mots de passe, la mise en œuvre appropriée des authentificateurs et la mise en œuvre appropriée des vérificateurs hors bande ou ponctuels.

Activer l'authentification multifacteur basée sur les rôles [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour appliquer l'authentification multifacteur (MFA) basée sur les `glide.authenticate.multifactor` rôles à tous les utilisateurs affectés à des rôles spécifiques.

Appliquez l'authentification multifacteur en fonction des rôles attribués à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » sont affectés à un utilisateur dans la liste des rôles multifacteur, MFA est appliquée.

- Définissez cette propriété sur **vrai** pour appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
- Attribuez la valeur **false** à cette propriété pour désactiver l'authentification multifacteur basée sur le rôle pour tous les utilisateurs affectés à des rôles spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multifactor`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Authentification
Objectif	Appliquez l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
Type	vrai/faux
Valeur recommandée	`true`
Dépendances de Sécurité	Activez **l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé à des données sensibles.
Références	Configurer les critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer l'authentification multifacteur basée sur les rôles [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour appliquer l'authentification multifacteur (MFA) basée sur les `glide.authenticate.multifactor` rôles à tous les utilisateurs affectés à des rôles spécifiques.

Appliquez l'authentification multifacteur en fonction des rôles attribués à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » sont affectés à un utilisateur dans la liste des rôles multifacteur, MFA est appliquée.

- Définissez cette propriété sur **vrai** pour appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
- Attribuez la valeur **false** à cette propriété pour désactiver l'authentification multifacteur basée sur le rôle pour tous les utilisateurs affectés à des rôles spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multifactor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Appliquez l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
Type	Booléen
Valeur recommandée	`true`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	Faux
Dépendances de Sécurité	Activez **l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé à des données sensibles.
Références	Configurer les critères multifacteur basés sur les rôles

Délai de verrouillage du contrôle pour les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et 2.0]

La `password_reset.request.max_attempt_window` propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit patienter avant de réinitialiser ou de changer son mot de passe après avoir dépassé le nombre maximal de tentatives infructueuses défini avec la `password_reset.request.max_attempt` propriété.

La `password_reset.request.max_attempt_window` propriété définit le nombre de minutes pendant lesquelles un utilisateur doit patienter avant de réinitialiser ou de changer son mot de passe après avoir dépassé le nombre maximal de tentatives infructueuses défini avec le `password_reset.request.max_attempt property`. Un petit nombre de minutes pour la `password_reset.request.max_attempt_window` propriété augmente le risque d'attaque par force brute réussie d'un mot de passe, car un plus grand nombre de tentatives de réinitialisation du mot de passe peuvent être effectuées. La valeur par défaut de 1440 minutes est recommandée.

Assurez-vous que la propriété `password_reset.request.max_attempt_window` est définie sur 1 440 ou plus.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.max_attempt_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique la période de verrouillage en minutes après l'atteinte du nombre maximal de tentatives infructueuses de réinitialisation du mot de passe.
Valeur recommandée	1440
Valeur par défaut	1440
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou moins, il est possible d'effectuer une opération de force brute du compte, car le compte ne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	sera pas verrouillé après un nombre maximal de tentatives d'authentification incorrectes.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mis à jour dans Centre de sécurité 1.3]

Utilisez la `glide.user.trusted_domain` propriété pour spécifier la liste séparée par des virgules des domaines de confiance utilisés dans la création des utilisateurs à partir des e-mails entrants.

Un administrateur peut définir une propriété d'e-mail pour créer automatiquement des utilisateurs à partir d'e-mails entrants. Si cette propriété est définie sur la valeur non sécurisée, l'instance crée automatiquement des utilisateurs à partir de l'e-mail entrant. Chaque utilisateur créé aura le même mot de passe codé en dur par défaut, ce qui facilite le contournement de l'authentification par force brute.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.pop3readerjob.create_caller`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Valeur recommandée	Faux
Valeur par défaut	Faux
Cote de risque de sécurité	5.4
Impact fonctionnel	Une fois cette propriété configurée, l'instance accepte uniquement les e-mails provenant de domaines de confiance. Si vous n'incluez pas le domaine dans la liste de confiance, cela a un impact sur les utilisateurs invités, car les comptes sont créés automatiquement.
Risque de sécurité	(Modéré) Si la propriété n'est pas activée, un attaquant peut utiliser une campagne d'usurpation d'adresse e-mail/spamming pour envoyer plusieurs e-mails, ce qui entraîne la création d'utilisateurs invités inutiles.
Références	Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver l'authentification sans mot de passe

Utilisez la propriété pour empêcher les `glide.login.no_blank_password` utilisateurs de se connecter à la Now Platform avec des mots de passe vides, ou en laissant le champ **Mot de passe** vide.

Même si l'administrateur attribue délibérément une valeur vide ou un mot de passe vide dans les enregistrements utilisateur, un utilisateur ne peut pas se connecter sans fournir une valeur dans le champ **Mot de passe** .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.login.no_blank_password`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour assurer une authentification forte comme parfois les noms d'utilisateur sont faciles à deviner au sein d'une organisation.
Valeur recommandée	vrai
Impact fonctionnel	Les opérations ne doivent pas utiliser de mots de passe vierges, car cela représente un risque de sécurité critique. Toutefois, s'il existe un cas valide pour une telle utilisation, une panne est possible. Les utilisateurs avec des mots de passe vides ne peuvent pas se connecter à l'instance.
Risque de sécurité	(Élevé) Un attaquant est capable de se connecter à l'instance avec les noms d'utilisateur par défaut, ou par un individu/groupe spécifique (généralement prénom.nom) sans mot de passe. Cela est considéré comme un risque de sécurité critique, car cela permettrait à un utilisateur public de violer la confidentialité et l'intégrité des données d'instance.

Désactiver les informations d'identification du mot de passe du propriétaire de ressource (ROPC) dans les attributions de jetons OAuth 2 [Nouveau dans Security Center 7.0]

Empêchez les informations d'identification du mot de passe du propriétaire de ressource (ROPC) d'accorder des jetons OAuth 2.

Par défaut, les informations d'identification du mot de passe du propriétaire de ressource (ROPC) sont autorisées à accorder des jetons OAuth 2 sur vos instances lorsqu'une application cliente demande directement un jeton d'accès à l'aide d'un nom d'utilisateur et d'un mot de passe. Lorsque la `glide.oauth.inbound.ropc.grant_type.disabled` valeur est définie sur **vrai**, ROPC est inactif et ne peut pas être utilisé pour accorder des jetons OAuth 2.

Assurez-vous que la `glide.oauth.inbound.ropc.grant_type.disabled` propriété système est définie sur **true**. Si la propriété n'existe pas dans la table Propriétés système [sys_properties], la valeur par défaut est **faux**. Si cette propriété existe sur cette table, elle est définie par défaut sur **false**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.oauth.inbound.ropc.grant_type.disabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Valeur de secours	Faux
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,3 • Score CVSS : faible • Lorsque la propriété est définie sur **faux**, l'utilisation de ROPC pour accorder des jetons OAuth 2 est autorisée. Le ROPC est considéré comme moins sécurisé que les autres flux d'authentification, car les informations d'identification de l'utilisateur sont exposées à l'application. Cela peut entraîner des vulnérabilités dans des situations où le client est compromis et souffre de faiblesses similaires à celles de l'authentification de base. OAuth 2.1 a déconseillé ROPC.
Impact fonctionnel	Lorsque la propriété est définie sur **vrai**, ROPC est inactif et ne peut pas être utilisé pour accorder des jetons OAuth 2. Cela empêche toutes les applications d'accéder à la plateforme en accordant le jeton OAuth 2 à l'aide de ROPC.
Dépendances et prérequis	Le module d'extension OAuth 2.0 (com.snc.platform.security.oauth) doit être actif.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Ne pas appliquer la politique de mot de passe lors de la connexion [Mis à jour dans Centre de sécurité 1.5 et supprimé dans la version 2.0]

Gérez la façon dont la complexité du mot de passe est traitée dans votre instance.

Si vous définissez la propriété `glide.apply.password_policy.on_login` sur faux, il n'y aura pas d'application de la complexité du mot de passe au moment de la connexion. Définir la propriété sur vrai renforce la complexité du mot de passe et entraîne des problèmes de conformité à la politique de l'organisation.

Selon les recommandations de l'ASVS 4.03 v2.1.9 :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

« Vérifiez qu'il n'y a pas de règles de composition de mot de passe limitant le type de caractères autorisés. Il ne devrait pas y avoir d'exigence de majuscules ou de minuscules ou de chiffres ou de caractères spéciaux. (C6)"

Au lieu d'appliquer la complexité du mot de passe, l'ASVS recommande d'appliquer une longueur minimale de 12 caractères pour la longueur du mot de passe.

Reportez-vous à l'authentification OWASP ASVS v4.0 .

En savoir plus

Attribut	Description
Nom de la configuration	`glide.apply.password_policy.on_login`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **vrai** peut rendre le mot de passe plus complexe et entraîner des problèmes de conformité de l'organisation.
Dépendances et prérequis	Aucun

Activer la récupération de compte [Mis à jour dans Centre de sécurité 1.3 et 1.5]

La `glide.sso.acr.enabled` propriété contrôle la fonctionnalité de récupération de compte.

Définissez `glide.sso.acr.enabled` sur la valeur recommandée **vrai** pour permettre une récupération de compte par userid possible. Définissez la valeur sur **faux** pour interdire la récupération de compte par userid.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sso.acr.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Contrôle la récupération de compte par fonctionnalité d'ID d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	True (par défaut)
Type de configuration	Booléen
Risque de sécurité	Critique (sans cette propriété activée, les utilisateurs ne seront pas autorisés à récupérer leur compte par ID d'utilisateur.
Cote de risque de sécurité	9.1
Références	Voir Récupération de compte (ACR) pour plus d'informations.

Activer CAPTCHA pour l'inscription du client

Réduisez le risque de demandes par des bots malveillants en activant CAPTCHA pour l'enregistrement des clients.

Utilisez la propriété système **sn_customerservice.captchaEnabled** pour déterminer si la validation CAPTCHA est activée pour l'inscription du client sur le portail Gestion du service clientèle. Utilisez la validation CAPTCHA pour empêcher les bots potentiellement malveillants de soumettre automatiquement des demandes contre une application.

Définissez la propriété système **sn_customerservice.captchaEnabled** sur **vrai** pour activer la validation CAPTCHA. Si la propriété ne figure pas dans la table Propriétés système [sys_properties], la valeur par défaut est **vrai**.

En savoir plus

Attribut	Description
Nom de la configuration technique	sn_customerservice.captchaEnabled
Applicabilité du module d'extension	Gestion du service clientèle
Risque de sécurité	La validation CAPTCHA permet d'empêcher les bots potentiellement malveillants de soumettre automatiquement des demandes contre une application.
Score du système de notation des vulnérabilités courantes (CVSS)	3.7
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Les utilisateurs qui s'inscrivent peuvent avoir une expérience négative en ayant à passer la validation CAPTCHA.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	**true**
Valeur de secours	**true**
Valeur recommandée	**true**

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer un contrôle de validation du mot de passe sur liste de refus

Gérez les mots de passe de la liste de refus dans la table Mot de passe exclu.

Utilisez la propriété pour surveiller les *glide.enable.blacklist_password* mots de passe de liste de refus. Lorsque la propriété est définie sur **Vrai**, le mot de passe de l'utilisateur est vérifié par rapport à une liste des mots de passe de la liste de refus pour l'empêcher d'utiliser un mot de passe provenant d'un ensemble de mots de passe violés. L'administrateur peut gérer la liste en insérant des mots de passe dans la table Mot de passe exclu.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.enable.blacklist_password*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Authentification
Dépendances et prérequis	Aucun
Références	Exclure les mots de passe via les politiques de mot de passe sur votre instance

Activer le Captcha pour l'inscription de l'utilisateur externe [mis à jour dans Centre de sécurité 1.3 et 1.5]

Contrôle *sn_ext_usr_reg.captchaEnabled* si CAPTCHA sera validé pour l'inscription de l'utilisateur externe.

Définissez *sn_ext_usr_reg.captchaEnabled* la valeur recommandée sur **vrai** pour éviter les attaques de création automatique de compte nécessitant CAPTCHA pour l'enregistrement d'un utilisateur externe. Définissez la valeur sur **faux** pour ne pas exiger CAPTCHA pour l'inscription de l'utilisateur externe.

En savoir plus

Attribut	Description
Nom de la propriété	*sn_ext_usr_reg.captchaEnabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Cette propriété est utilisée pour activer ou désactiver la validation CAPTCHA lors de l'enregistrement d'un utilisateur externe sur des portails tels que CSP, Communauté. Cette fonction est également utilisée dans les applications de stockage telles que VAM et CSM Guest Walkup pour activer/désactiver le captcha.
Valeur recommandée	Vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Booléen
Risque de sécurité	(Faible) La propriété contrôle l'activation de CAPTCHA dans l'inscription de l'utilisateur externe. Une valeur non idéale peut entraîner une vulnérabilité de la sécurité.
Cote de risque de sécurité	3.7

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Activer CAPTCHA dans Réinitialisation du mot de passe

Utilisez la propriété pour activer ou désactiver l'exigence `password_reset.captcha.ignore` d'une contestation CAPTCHA lorsqu'un utilisateur réinitialise son mot de passe.

Définissez `password_reset.captcha.ignore` la valeur recommandée sur **faux** pour exiger un défi CAPTCHA pour qu'un utilisateur réinitialise son mot de passe. Définissez la valeur sur **vrai** pour ignorer l'option CAPTCHA pour une réinitialisation du mot de passe.

Les CAPTCHA aident à prévenir les attaques d'automatisation en invitant l'utilisateur à un défi-réponse auquel les systèmes automatisés ne répondent pas facilement. Si CAPTCHA est désactivé, un attaquant peut avoir plus de succès lors d'attaques automatisées contre la fonctionnalité de réinitialisation de mot de passe.

Remarque :
Cette propriété est utilisée uniquement pour l'automatisation de la réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.captcha.ignore`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Cette propriété permet d'activer ou de désactiver la validation CAPTCHA pendant la réinitialisation du mot de passe.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Modéré) Une valeur non idéale peut entraîner une vulnérabilité de la sécurité.
Cote de risque de sécurité	5.5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Activer l'OTP d'e-mail pour l'authentification multifacteur

Gérez la façon dont l'authentification à deux facteurs est appliquée sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez cette`glide.authenticate.multifactor.email.otp.enabled` propriété pour contrôler si un jeton pour l'authentification à deux facteurs est envoyé par e-mail. L'e-mail est considéré comme un facteur MFA faible auquel un attaquant est plus susceptible d'accéder pour contourner l'authentification multifacteur. En définissant cette propriété sur **faux**, le risque qu'un attaquant contourne la MFA lorsqu'il a compromis le mot de passe d'un utilisateur est réduit.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.multifactor.email.otp.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : définir cette propriété sur **faux** réduit le risque qu'un acteur malveillant contourne l'authentification à deux facteurs.
Dépendances et prérequis	Aucun
Références	L'e-mail en tant que facteur MFA

Activer les contrôles de la politique de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 2.0]

Utilisez la propriété **glide.enable.password_policy** pour activer les vérifications de la politique de mot de passe chaque fois qu'un utilisateur modifie son mot de passe à l'aide de l'interface utilisateur.

Pour définir la politique de mot de passe à utiliser une fois cette propriété activée, reportez-vous à la section Activer les politiques de mot de passe sur votre instance. Assurez-vous que la propriété `glide.enable.password_policy` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

Remarque :
La **glide.enable.password_policy** ne s'applique pas lorsqu'un administrateur modifie un mot de passe ou ajoute un utilisateur via un script.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.enable.password_policy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Pour appliquer la politique de mot de passe au moment du changement de mot de passe.
Valeur recommandée	vrai (pour les mots de passe plus puissants)
Cote de risque de sécurité	7.4
Impact fonctionnel	Définir la propriété sur vrai active les vérifications de la politique de mot de passe lorsqu'un utilisateur réinitialise son mot de passe.
Risque de sécurité	(Modéré) Sans politique de mot de passe, un utilisateur peut créer un mot de passe faible, ce qui augmente la probabilité qu'un adversaire accède à l'instance.

Étapes de configuration

Si vous configurez ce paramètre dans la page Configuration de la conformité à la sécurisation renforcée dans le Centre de sécurité de l'instance :

1. Sous **Moyen**, sélectionnez **Gestion des sessions**.
2. Dans le paramètre **Activer la vérification de la politique de réinitialisation du mot de passe** , sélectionnez **Moyen** pour les mots de passe de niveau moyen ou **Fort** pour les mots de passe plus robustes et plus forts. La sélection de l'une de ces options définit la propriété **glide.enable.password_policy** sur true et lance un workflow qui met automatiquement à jour votre politique de mot de passe.

En outre, vous pouvez définir la propriété système pour activer les `glide.apply.password_policy.on_login` vérifications de la politique de mot de passe au moment de la connexion.

Activer l'accès à la session basé sur des politiques pour mobile [Nouveau dans Security Center 1.5]

Utilisez le module d'extension Zero Trust - Policy Based Session Access pour contrôler si les rôles des utilisateurs s'authentifiant via une application mobile seront réduits.

Le module d'extension Zero Trust - Policy Based Session Access permet aux administrateurs de sécurité de réduire l'accès des utilisateurs dans une session en fonction de paramètres tels que l'adresse IP, l'emplacement, d'identifier les attributs de fournisseur et les attributs d'utilisateur avec des politiques d'authentification adaptative. Lorsque ce module d'extension est activé ou défini sur vrai, les rôles des utilisateurs qui s'authentifient via un appareil mobile sont restreints en fonction des politiques du module d'extension. Les administrateurs d'instance peuvent souhaiter restreindre l'accès avec des privilèges élevés lorsque les utilisateurs s'authentifient via un équipement mobile, car cela pourrait indiquer un environnement dangereux pour des opérations sensibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.mobile.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,7 • Score CVSS : moyen • Détails du risque de sécurité : si ce paramètre de sécurisation renforcée est défini sur vrai, l'accès à la session basé sur des politiques est appliqué sur l'instance pour les connexions mobiles, et les utilisateurs qui ne proviennent pas d'un environnement approuvé ou qui n'utilisent pas d'appareils approuvés verront leurs rôles avec des privilèges réduits. Vrai est le paramètre sécurisé. Si ce paramètre est configuré sur faux, l'accès à la session basé sur des politiques est désactivé et les utilisateurs continueront à disposer de rôles complets, y compris les rôles avec des privilèges élevés comme administrateur en permanence.
Dépendances et prérequis	Aucun
Impact fonctionnel	Si l'administrateur a configuré la politique d'accès à la session sur l'instance, les rôles des utilisateurs seront réduits après la connexion mobile s'ils ne proviennent pas d'un environnement approuvé ou n'utilisent pas d'appareil approuvé.
Références	Authentification adaptative

Traduction automatique

Activer l'état du relais dans les demandes SAML pour prévenir les attaques par relecture

Réduisez le risque d'attaques par relecture en activant l'état de relais dans les demandes SAML afin de prévenir les attaques par relecture.

Protégez-vous contre les attaques par relecture SAML à l'aide de la propriété système **glide.authenticate.sso.saml2.enable_relay_state_with_id** . Lorsque cette propriété est définie sur **vrai**, le paramètre d'état du relais contient le sys_id d'un enregistrement dans la table Paramètres de demande de SSO à fournisseurs multiples [multisso_request_parameter], vers laquelle l'URL de l'état du relais redirige.

Définissez la propriété système **glide.authenticate.sso.saml2.enable_relay_state_with_id** sur **vrai**. Cela permet d'empêcher les attaquants qui ont obtenu l'accès à une demande SAML d'accéder à votre instance en soumettant à nouveau une demande valide.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.authenticate.sso.saml2.enable_relay_state_with_id
Applicabilité du module d'extension	Module d'extension SSO de plusieurs fournisseurs (com.snc.integration.sso.multi.installer)
Risque de sécurité	L'état du relais activé par cette propriété système permet de protéger votre instance contre les attaques par relecture. L'activation de la propriété permet d'empêcher les attaquants qui ont obtenu l'accès à une demande SAML d'accéder à votre instance en soumettant à nouveau une demande valide.
Score du système de notation des vulnérabilités courantes (CVSS)	3.8
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, l'état du relais d'une demande SAML contient l'sys_id d'un enregistrement dans la table Paramètres de demande MultiSSO [multisso_request_parameter], qui contient l'URL d'état du relais vers laquelle la redirection s'effectue.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	vrai
Valeur de secours	Faux
Valeur recommandée	vrai

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la notification du code SMS pour l'inscription et la vérification [Mis à jour dans Centre de sécurité 1.3]

La*password_reset.sms.use_notify* propriété contrôle l'utilisation des notifications de code SMS pour la réinitialisation du mot de passe.

Si la *password_reset.sms.use_notify* propriété est définie sur la valeur recommandée **vrai**, l'utilisateur est invité à effectuer une réinitialisation du mot de passe à l'aide de la vérification par SMS et de l'inscription d'un nouvel appareil, qui est plus sécurisée que l'e-mail.

En savoir plus

Attribut	Description
Nom de la configuration	*password_reset.sms.use_notify*
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	booelan
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : si vous définissez cette propriété sur**faux** , l'e-mail devient la méthode par défaut de récupération de mot de passe, qui est moins sécurisée que les SMS.
Dépendances et prérequis	Aucun

Activer SSL dans l'authentification LDAP [Mis à jour dans Centre de sécurité 1.5 et 2.0]

Gérez le chiffrement des demandes d'authentification LDAP sur votre instance.

Utilisez lapropriété permettant d'activer ou de désactiver le `glide.ldap.use.ssl` chiffrement TLS pour les demandes d'authentification LDAP envoyées sur le réseau. Si cette propriété n'est pas définie sur la valeur conseillée **true**, LDAP Authentication est susceptible d'être victime d'une attaque de l'intercepteur du milieu.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ldap.use.ssl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **faux** rend LDAP Authentication vulnérable à une attaque de l'intercepteur du milieu.
Dépendances et prérequis	Aucun
Références	Intégration du protocole LDAP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les exigences actuelles de conformité à la politique de mot de passe lors de la connexion

Réduisez le risque de connexion par force brute au compte en appliquant les exigences actuelles de conformité à la politique de mot de passe lors de la connexion.

Empêchez les utilisateurs interactifs de se connecter à l'instance avec des mots de passe qui ne répondent pas aux exigences actuelles de l'administrateur à l'aide de la propriété système **glide.apply.password_policy.on_login** .

Définissez la propriété système **glide.apply.password_policy.on_login** sur **vrai** pour appliquer les exigences actuelles de conformité à la politique de mot de passe. Si cette propriété n'existe pas dans la table Propriétés système [sys_properties], la valeur par défaut est **faux**.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.apply.password_policy.on_login
Applicabilité du module d'extension	Aucun
Risque de sécurité	Les utilisateurs interactifs peuvent continuer à se connecter à l'instance avec des mots de passe qui ne répondent pas aux exigences actuelles de l'administrateur. Cela peut signifier que les utilisateurs ont des mots de passe faibles qui ne répondent pas aux exigences de sécurité à jour, ce qui peut entraîner un risque accru de connexions de compte par force brute par un utilisateur malveillant.
Score du système de notation des vulnérabilités courantes (CVSS)	4.4
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	Si les mots de passe existants ne sont pas conformes à votre politique de mot de passe actuelle, l'activation de cette propriété oblige les utilisateurs à changer les mots de passe lors de leur prochaine connexion. Cette propriété est automatiquement définie sur **false**. Définir la valeur sur **vrai** applique une politique de mot de passe lors de la connexion. **Remarque :** L'activation de cette propriété peut forcer un nombre important d'utilisateurs qui ne sont pas en conformité avec la nouvelle politique de mot de passe à changer leurs mots de passe.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	Faux
Valeur de secours	Faux
Valeur recommandée	vrai

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les exigences relatives au chiffrement de l'appareil et au code d'accès [nouveau dans Security Center 1.3]

La *glide.sg.device_encryption_enabled* propriété applique le chiffrement de la norme fédérale de traitement de l'information (FIPS 140-2). Le chiffrement et le code d'accès des appareils mobiles garantissent qu'un utilisateur non autorisé ne peut pas accéder au contenu d'un appareil, même si celui-ci est physiquement en sa possession.

Lorsque *glide.sg.device_encryption_enabled* cette option est définie sur vrai, l'application mobile ServiceNow vérifie que le chiffrement de l'appareil et le code d'accès de l'appareil sont activés.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.sg.device_encryption_enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : si le chiffrement ou le code d'accès n'est pas activé, l'utilisateur ne sera pas autorisé à se connecter à l'instance sur mobile
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, l'application mobile vérifie si le chiffrement de l'appareil est activé. Si le chiffrement n'est pas activé, les utilisateurs ne seront pas autorisés à se connecter à l'instance actuelle sur mobile. Les utilisateurs sont déconnectés et voient le message d'avertissement suivant, leur suggérant de définir un code PIN d'appareil ou de chiffrer l'appareil et d'essayer de se connecter à nouveau. You were logged out You need a passcode in order to use this instance on this device. Go to your device's settings to set one up

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limiter les tentatives de réinitialisation du mot de passe non valide [Mis à jour dans Centre de sécurité 1.3 et mis à jour dans la version 2.0]

Cette fonction *password_reset.request.max_attempt* est utilisée pour contrôler le nombre maximal de tentatives infructueuses qu'un utilisateur peut réinitialiser ou changer son mot de passe avant d'être verrouillé pour une période donnée.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.request.max_attempt*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique le nombre maximal de tentatives infructueuses de réinitialisation du mot de passe qui peuvent être effectuées avant que l'utilisateur ne soit bloqué hors du processus de réinitialisation du mot de passe. La période de verrouillage est déterminée par la valeur dans *password_reset.request.max_attempt_window*.
Valeur recommandée	Définir sur une valeur entière positive inférieure à trois. La valeur par défaut est de **3**. Lorsque vous déterminez la limite de la plage supérieure de la propriété, tenez compte de la tâche que l'utilisateur effectue.
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de « **3** » ou sur une autre valeur faible raisonnable, il peut être possible d'effectuer une attaque par force brute contre le processus de réinitialisation du mot de passe.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Gestion du délai de déverrouillage après des échecs de connexion [Mis à jour dans Centre de sécurité 1.3]

Deux actions de script sont disponibles pour permettre à un administrateur de site de gérer le nombre de fois qu'un utilisateur peut fournir un mot de passe incorrect avant d'être bloqué par le ServiceNow AI Platform. Vous pouvez activer l'une ou l'autre de ces actions de script pour gérer les échecs de tentative de connexion.

En savoir plus

Attribut	Description
Nom de la propriété/du module d'extension	N/A
Type de configuration	Politique système > Actions des scripts
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour appliquer une politique stricte en cas d'échec de tentative de connexion afin d'éviter la force brute des informations d'identification.
Valeur recommandée	Actif
Cote de risque de sécurité	7.3
Impact fonctionnel	Cette correction permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur malveillant. Aucun impact sur les fonctionnalités, uniquement un changement de l'expérience utilisateur.
Risque de sécurité	(Modéré) Appliquez une stratégie de journalisation et d'audit définie afin de pouvoir identifier les activités suspectes et agir en temps opportun.

Étapes de configuration

1. Accédez à la **Politique système** > **Actions des scripts.**
2. Recherchez le nom *`*SNC User`*.
3. Pour activer la gestion des échecs de tentatives de connexion, changez l'état *`SNC User Lockout Check with Auto Unlock`* actif des actions des scripts ou *`SNC User Lockout Check`* de **faux** à **vrai**.
4. Pour réinitialiser le compteur d'échecs de connexion après une connexion réussie, vous pouvez activer l'action des *`SNC User Clear`* scripts.

Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion [Mis à jour dans Centre de sécurité 1.3]

Deux actions de script sont disponibles pour permettre à un administrateur de site de gérer le nombre de fois qu'un utilisateur peut fournir un mot de passe incorrect avant d'être bloqué par le ServiceNow AI Platform. Vous pouvez activer l'une ou l'autre de ces actions de script pour gérer les échecs de tentative de connexion.

Protégez votre instance contre les attaques par force brute en définissant une période pendant laquelle un utilisateur ne peut pas tenter de se connecter après avoir été verrouillé. La propriété système **glide.user.unlock_timeout_in_mins** déverrouille le compte d'utilisateur après la période spécifiée dans sa valeur. Si aucune valeur n'est spécifiée, votre instance déverrouille le compte d'utilisateur après la période par défaut de 15 minutes.

Définissez la valeur de la propriété système **glide.user.unlock_timeout_in_mins** sur un minimum de **15**. Si **glide.user.unlock_timeout_in_mins n'existe** pas, la durée de verrouillage par défaut est fixée à 15 minutes.

Assurez-vous que l'action **des scripts Vérification du verrouillage de l'utilisateur SNC avec déverrouillage automatique** (qui se trouve dans la table Action des scripts [sysevent_script_action]) est présente et active. L'action **de script Vérification de verrouillage de l'utilisateur SNC avec déverrouillage automatique** est installée avec le module d'extension Paramètres de sécurité élevée (com.glide.high_security).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	• glide.user.unlock_timeout_in_mins (propriété système) • sysevent_script_action (Action des scripts)
Type de configuration	Politique système > Actions des scripts
Catégorie	Authentification
Objectif	Pour appliquer une politique stricte en cas d'échec de tentative de connexion afin d'éviter la force brute des informations d'identification.
Valeur recommandée	• **15** pour la propriété système **glide.user.unlock_timeout_in_mins** • **Actif** pour le **SNC Vérification du verrouillage de l'utilisateur avec l'action des scripts Déverrouillage automatique** .
Impact fonctionnel	Cette correction permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur malveillant. Aucun impact sur les fonctionnalités, uniquement un changement de l'expérience utilisateur.
Risque de sécurité	• Score de gravité : 6,8 • Détails du risque de sécurité : si la propriété n'est pas configurée sur une valeur sécurisée et que la durée du verrouillage n'est pas activée, il peut être plus facile d'effectuer une attaque par force brute des connexions de compte dans un délai plus rapide. Cela peut permettre à un utilisateur malveillant d'obtenir un accès non autorisé à l'instance. L'impact sur l'instance sera limité aux privilégiés de la connexion de l'utilisateur affecté en force brute.

Étapes de configuration

1. Accédez à la **Politique système** > **Actions des scripts.**
2. Recherchez le nom *`*SNC User`*.
3. Pour activer la gestion des échecs de tentatives de connexion, changez l'état *`SNC User Lockout Check with Auto Unlock`* actif des actions des scripts ou *`SNC User Lockout Check`* de **faux** à **vrai**.
4. Pour réinitialiser le compteur d'échecs de connexion après une connexion réussie, vous pouvez activer l'action des *`SNC User Clear`* scripts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

La *password_reset.request.retry_window* propriété contrôle le nombre de minutes avant l'actualisation du nombre de tentatives de réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.request.retry_window*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique la durée, en minutes, avant que le nombre de tentatives de mot de passe ne soit actualisé à partir de la dernière demande avant que le nombre de nouvelles tentatives ne soit remis à zéro.
Valeur recommandée	Défini sur une valeur entière positive égale ou supérieure à **1 440** . La valeur par défaut est **1 440** minutes.
Type de configuration	Valeurs entières positives.
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou plus, il peut être possible d'effectuer un processus de réinitialisation du mot de passe en force brute du compte.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

La *password_reset.request.unlock_window* propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour lancer une demande de réinitialisation suite à la dernière action de déverrouillage de compte réussie.

Cette propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour lancer une demande de réinitialisation après le dernier déverrouillage de compte réussi. Si *password_reset.request.unlock_window* elle n'est pas définie sur la valeur recommandée de 1 440 ou plus, cela augmente la possibilité pour un acteur malveillant d'effectuer une attaque par force brute du mot de passe de l'utilisateur à l'aide d'outils automatisés.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.request.unlock_window*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit patienter après avoir réussi à réinitialiser le mot de passe pour réinitialiser le mot de passe.
Valeur recommandée	1440
Valeur par défaut	1440
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur conseillée de 1 440 ou supérieure, cela augmente la possibilité pour un acteur malveillant d'effectuer une attaque par force brute pour l'accès par mot de passe à l'aide d'outils automatiques.
Cote de risque de sécurité	5.9
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Maximiser la complexité du SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

La *password_reset.sms.default_complexity* propriété contrôle la taille minimale requise pour la vérification du code SMS pendant la réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.sms.default_complexity*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique la taille de vérification du code SMS requise pendant la réinitialisation du mot de passe.
Valeur recommandée	6
Valeur par défaut	4
Type de configuration	Valeur entière supérieure à zéro
Risque de sécurité	(Faible) Si la propriété n'est pas définie sur la valeur recommandée, un jeton de validation SMS faible est utilisé. Cela augmente la possibilité de deviner des jetons, ce qui pourrait conduire à la prise de contrôle des comptes.
Cote de risque de sécurité	3.8

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

Gérez la durée d'attente en minutes qu'un utilisateur doit attendre avant de pouvoir demander un nouveau code de réinitialisation du mot de passe.

Si cette propriété n'est pas définie sur la valeur recommandée de **2** minutes ou plus, un utilisateur malveillant peut alors lancer de nombreux codes de réinitialisation de mots de passe dans une brève période de temps. Cela augmente les chances qu'un acteur malveillant prédise le code de réinitialisation par SMS.

En savoir plus

Attribut	Description
Nom de la configuration	*password_reset.sms.pause_window*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	2
Valeur par défaut	2
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,8 • Score CVSS : moyen • Détails du risque de sécurité : assurez-vous que *password_reset.sms.pause_window* est défini sur une valeur de 2 ou plus.
Dépendances et prérequis	Aucun

Maximiser la durée du délai de vérification de la réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

Configurez le délai, en millisecondes, qu'un utilisateur doit attendre avant de soumettre une nouvelle demande de réinitialisation du mot de passe.

Un acteur malveillant pourrait tenter d'effectuer une attaque par force brute des identifiants de connexion en utilisant des outils d'automatisation tels que les bots, contre lesquels la propriété de **délai de vérification de la réinitialisation du mot de passe** permet de se défendre. La valeur de la propriété représente le délai, en millisecondes, qu'un utilisateur doit attendre avant de pouvoir demander la réinitialisation du mot de passe. Si cette propriété n'est pas définie sur la valeur recommandée de **1 000** ou plus, la connexion est plus vulnérable aux attaques par force brute.

En savoir plus

Attribut	Description
Nom de la configuration	*password_reset.verification.delay*
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	chaîne
Valeur recommandée	1 000
Valeur par défaut	1 000
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : définir la valeur de la propriété sur moins de 1 000 rend votre connexion plus vulnérable aux attaques par force brute.
Dépendances et prérequis	Aucun
Références	Configurer le mot de passe d'un utilisateur

Minimiser la durée d'expiration du lien d'inscription de l'utilisateur externe [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Gérez le nombre de jours d'accès à un lien d'inscription.

Utilisez la *sn_ext_usr_reg.Reg_link_expiration_days* propriété pour gérer qui peut accéder à un lien d'inscription. Si le lien est défini sur la valeur recommandée de **3**, un lien d'inscription peut être utilisé par une autre personne que l'utilisateur prévu si le lien est découvert à une date ultérieure.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_ext_usr_reg.Reg_link_expiration_days*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Entier
Valeur recommandée	3
Valeur par défaut	3
Catégorie	Authentification
Risque de sécurité	• Score de gravité : moyenne • Score CVSS : 6,6 • Détails du risque de sécurité : ne pas définir cette propriété sur l'entier 3 peut entraîner l'utilisation du lien d'inscription par un utilisateur non prévu.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour [Mis à jour dans Centre de sécurité 1.3]

Gérez le nombre maximal de codes SMS envoyés quotidiennement pour vérification par utilisateur.

La*password_reset.sms.max_per_day* propriété représente le nombre maximal de codes SMS qui peuvent être envoyés quotidiennement pour vérification par un utilisateur.

En savoir plus

Attribut	Description
Nom de la configuration	*password_reset.sms.max_per_day*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	10
Valeur par défaut	10
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée de **10** ou moins, il est plus facile d'effectuer une attaque par force brute du code SMS.
Dépendances et prérequis	Aucun

Minimiser les tentatives de connexion échouées pour les sessions d'assurance élevée

Diminuez la probabilité d'une attaque par force brute en minimisant les échecs de tentatives de connexion pour les sessions d'assurance élevée.

Utilisez la propriété système **glide.zta.high_assurance.session.max.login.failed_attempts** pour limiter le nombre d'échecs de tentatives d'authentification autorisés avant que les utilisateurs ne soient déconnectés lors d'une nouvelle authentification via l'authentification continue.

Définissez la valeur de cette propriété système sur une valeur faible (par exemple, 5) pour réduire la probabilité d'une attaque par force brute.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.zta.high_assurance.session.max.login.failed_attempts
Applicabilité du module d'extension	Authentification Zero Trust - continue (com.snc.zero_trust_continuous_authentication)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	Un nombre élevé de tentatives d'authentification autorisées augmente la probabilité d'une attaque par force brute.
Score du système de notation des vulnérabilités courantes (CVSS)	3.3
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Les utilisateurs sont déconnectés de leurs sessions après le nombre d'échecs d'authentification sélectionnés dans la propriété.
Dépendances et prérequis	Aucun
Type de données	Entier
Valeur de système de base	5
Valeur de secours	5
Valeur recommandée	5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée d'expiration de la demande de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

Désigne la période, en minutes, `password_reset.request.expiry` pendant laquelle un utilisateur doit effectuer le processus de réinitialisation du mot de passe.

Remarque :
Le paramètre de la propriété prévaut sur le paramètre de `glide.pwd_reset.onetime.token.validity`la `password_reset.request.expiry` propriété qui a une valeur par défaut de 12 heures.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.expiry`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique la période en minutes pendant laquelle un utilisateur doit effectuer le processus de réinitialisation du mot de passe.
Valeur recommandée	Défini sur un nombre entier inférieur ou **égal à 10** . La valeur par défaut est de 10.
Type de configuration	Valeurs entières
Risque de sécurité	(Modéré) Si la propriété n'est pas définie sur la valeur conseillée de 10 ou moins, cela augmente la possibilité pour quelqu'un d'autre de deviner et d'utiliser la demande et de tenter de réinitialiser le mot de passe.
Cote de risque de sécurité	4.2

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée de la fenêtre de succès de demande de réinitialisation de mot de passe [Mis à jour dans Securty Center 1.3]

La *password_reset.request.success_window* propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit patienter avant de réinitialiser ou de changer à nouveau son mot de passe après avoir réinitialisé le mot de passe. L'utilisateur sera empêché de réinitialiser à nouveau le mot de passe pour la durée spécifiée.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.request.success_window*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit patienter après avoir réussi à réinitialiser le mot de passe pour réinitialiser le mot de passe.
Valeur recommandée	1440
Valeur par défaut	1440
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou moins, il est alors plus probable qu'une autre personne abuse de la fonctionnalité de réinitialisation du mot de passe pour obtenir un accès non autorisé à un compte utilisateur.
Cote de risque de sécurité	4.9
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée d'expiration de SMS de réinitialisation du mot de passe [Mis à jour dans Centre de sécurité 1.3]

Contrôlez le nombre de minutes restantes avant l'expiration du code SMS.

La*password_reset.sms.expiry* propriété représente le nombre de minutes restantes avant l'expiration du code SMS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`password_reset.sms.expiry`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	5
Valeur par défaut	5
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,6 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée de **5** ou moins, les chances qu'un acteur malveillant devine et utilise le code SMS pour réinitialiser le mot de passe augmentent.
Dépendances et prérequis	Aucun

Minimiser la durée de vie unique du vérificateur hors bande [Mis à jour dans Centre de sécurité 1.3]

Gérez la durée des vérificateurs hors bande.

Un vérificateur hors bande est une méthode de livraison alternative pour les situations de code à usage unique. Par exemple, la réinitialisation d'un jeton multifacteur. Si cette méthode est activée par les administrateurs dans le module d'extension Authentification multifacteur , un code à usage unique est envoyé par e-mail. Définissez des vérificateurs hors bande uniques pour qu'ils expirent après 10 minutes pour limiter la fenêtre de validité. Une fenêtre de temps plus longue laisse plus de temps pour que le code soit compromis par des moyens illicites tels que le phishing, l'ingénierie sociale ou les attaques par shoulder-surfing.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.multifactor.onetime.code.validity`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	10
Valeur par défaut	10
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : configurez les vérificateurs hors bande uniques pour qu'ils expirent au bout de 10 minutes. Tout ce qui est plus long augmente le risque que le code soit compromis par un acteur malveillant.
Dépendances et prérequis	Authentification multifacteur
Références	Critères d'authentification multifacteur

Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Configurez cette propriété pour ajouter une période de grâce au cours de laquelle les demandes et réponses SAML sont considérées comme valides.

Cette propriété ajoute une période de grâce au cours de laquelle les demandes et réponses SAML sont considérées comme valides. La valeur de la propriété représente le nombre de secondes à ajouter aux `NotBeforeNotOnOrAfter` contraintes et pour tenir compte des différences de temps entre l'horloge du fournisseur d'identité (IdP) et celle du fournisseur de service (SP). Ces contraintes protègent contre les attaques par rejeu en refusant les demandes qui ne sont pas effectuées dans le délai spécifié. Si les horloges IdP et SP sont très différentes, la latence du réseau peut entraîner le refus de l'autorisation de la demande SAML.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.sso.saml2.clockskew`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	moins de 60
Valeur par défaut	180
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : définir la propriété sur une valeur de 60 ou plus peut empêcher les contraintes de se défendre contre les attaques par relecture.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe [supprimé dans Centre de sécurité 1.5]

Utilisez cettepropriété pour permettre aux utilisateurs finaux de réinitialiser ou de changer les mots de passe à l'aide d'un processus en libre-service.

Cette propriété permet à un utilisateur final de réinitialiser ou de modifier un mot de passe à l'aide d'un processus en libre-service. Votre organisation peut également implémenter un processus qui nécessite qu'un agent du Centre de services réinitialise les mots de passe des utilisateurs finaux. Si un processus de changement ou de réinitialisation du mot de passe n'informe pas les utilisateurs de la mise à jour du mot de passe, un acteur malveillant peut être en mesure de verrouiller l'accès à leur compte à leur insu. Cela donnerait à l'acteur malveillant plus de temps pour effectuer des activités malveillantes. Assurez-vous que le processus de réinitialisation du mot de passe avertit les utilisateurs du changement ou de la réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la configuration	`pwd_process.change, pwd_process.reset`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : un acteur malveillant peut être en mesure de verrouiller un utilisateur hors de son compte à son insu si aucune notification ne lui est envoyée lorsqu'un changement de mot de passe est réinitialisé.
Dépendances et prérequis	Aucun

Réduire les contournements autorisés pour la configuration multifacteur

Réduisez la fenêtre de temps pendant laquelle un compte risque d'être compromis en réduisant les contournements autorisés pour la configuration multifacteur.

Réduisez le nombre de fois où un utilisateur peut ignorer l'exigence de configuration du code secret multifacteur afin de réduire la fenêtre pendant laquelle un compte risque d'être compromis. L'authentification multifacteur (MFA) protège contre les attaques liées aux mots de passe ou les mots de passe faibles en exigeant une forme de vérification supplémentaire. Réduire la durée pendant laquelle un utilisateur peut ignorer cette configuration réduit cette vulnérabilité.

Définissez la propriété système **glide.authenticate.multifactor.setup.bypass.count** sur **0** pour empêcher les utilisateurs d'ignorer la configuration du code secret multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.authenticate.multifactor.setup.bypass.count
Applicabilité du module d'extension	Aucun.
Risque de sécurité	L'authentification multifacteur protège contre les attaques liées aux mots de passe ou les mots de passe faibles en exigeant une forme de vérification supplémentaire. Un nombre élevé de contournements de configuration multifacteur autorisés augmente le risque de compromission du compte, car le compte n'est pas protégé par multifacteur. Un petit nombre de contournements autorisés réduit cette fenêtre de temps.
Score du système de notation des vulnérabilités courantes (CVSS)	3.9
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Les utilisateurs ne sont pas autorisés à se connecter à une instance sans configurer la MFA s'ils ont dépassé le nombre de connexions spécifiées dans la propriété.
Dépendances et prérequis	Aucun
Type de données	Entier
Valeur de système de base	0
Valeur de secours	0
Valeur recommandée	0

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Supprimer les informations d'identification de la page d'accueil

Modifiez le contenu par défaut sur la page d'accueil pour supprimer les informations d'identification par défaut.

Deux enregistrements **Comment se connecter** sont installés dans le cadre des données de démonstration du module d'extension CMS.

Remarque :
Si vous n'installez pas les données de démonstration pour une instance, ces enregistrements n'existent pas. Dans ce cas, la configuration est considérée comme conforme à la norme de sécurité conformément aux pratiques de sécurité recommandées.

En savoir plus

Attribut	Description
Nom	*How to login*
Type de configuration	Tableau : sys_home

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Authentification
Objectif	Pour supprimer les informations d'identification par défaut de la page d'accueil qui ont été ajoutées avec les données de démonstration.
Valeur recommandée	Faux ou nul si aucune donnée de démonstration n'a été utilisée.
Valeur par défaut	Aucun. Il s'agit d'une configuration de table, pas d'une propriété Glide. Par conséquent, il n'y a pas de valeur pour la valeur par défaut.
Type de configuration	Booléen
Risque de sécurité	(Modéré) Des données de démonstration sont fournies pour le module d'extension CMS, qui comprend deux mots de passe par défaut inclus sur la page d'accueil. Si elle n'est pas supprimée, un attaquant non autorisé peut accéder à l'instance.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Welcome pages

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger un captcha pour l'expérience de visite d'un invité dans l'application Service clientèle [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Le captcha pour l'expérience de visite des invités empêche les utilisateurs invités non authentifiés de créer des réservations en exigeant qu'ils effectuent une vérification captcha.

En savoir plus

Attribut	Description
Nom de la configuration	`sn_guest_walkup_cs.captcha.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	vrai
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : si le captcha n'est pas activé, cela peut entraîner la création automatisée de rendez-vous indésirables pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	submerger le système ou remplir toutes les places de réservation disponibles, créant ainsi une attaque par déni de service (DoS).
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété active ou désactive le captcha sur les widgets d'enregistrement de visite d'invité CSM. Par défaut, elle est définie sur vrai.

Exiger le brouillage de l'interface utilisateur de l'application mobile classique [Mis à jour dans Centre de sécurité 1.3]

Utilisez la *glide.ui.m.blur_ui_when_backgrounded* propriété pour masquer tous les champs de l'instantané lors de l'enregistrement de l'image en processus d'arrière-plan.

Sur les appareils Android, le système d'exploitation Android prend une capture d'écran pour l'utiliser dans le menu des tâches récentes lorsque l'application est envoyée en arrière-plan. Les utilisateurs peuvent également prendre des captures d'écran manuelles de l'application, qui sont stockées publiquement sur l'appareil.

Sur les appareils iOS, le système d'exploitation iOS permet également aux applications d'enregistrer un fichier image. Ce fichier représente le dernier écran vu par l'utilisateur lorsque l'application est envoyée en arrière-plan. Bien que l'intention soit de fournir une meilleure expérience utilisateur, cela crée également un risque de sécurité car les images sont enregistrées sous forme de fichiers image PNG.

Remarque :
Ce paramètre ou cette configuration est basé sur l'instance. L'utilisateur doit donc se connecter à l'instance avec la propriété configurée.

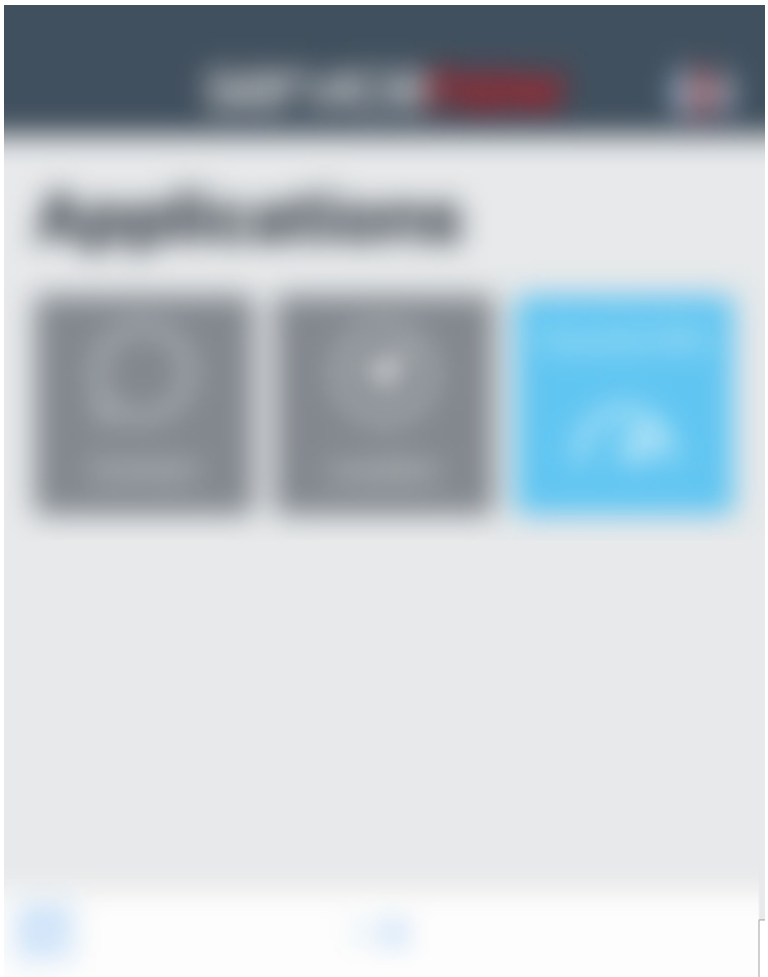
Pour masquer tous les champs de l'instantané dans l'application ServiceNow Classic, voir Configurer l'option de floutage de l'application pour améliorer la sécurité .

Exemple

Lorsque vous définissez cette propriété sur true, l'application background est brouillée pour les appareils iOS et bloquée pour les appareils iOS Android.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En savoir plus

Attribut	Description
Nom de la propriété/du module d'extension	`glide.ui.m.blur_ui_when_backgrounded`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Pour masquer tous les champs de l'instantané lors de l'enregistrement de l'image pendant le processus d'arrière-plan.
Valeur recommandée	vrai
Cote de risque de sécurité	2.4
Impact fonctionnel	Si la `glide.ui.m.blur_ui_when_backgrounded` propriété est définie sur true, les applications natives utilisent le paramètre défini sur le serveur pour brouiller l'écran lorsque l'application passe en arrière-plan.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Il brouille les captures d'écran prises par iOS et Android lorsque l'application entre en arrière-plan. • L'expérience utilisateur peut être affectée négativement, car il ne sera pas en mesure de voir le contenu lorsque l'application est envoyée en arrière-plan.
Risque de sécurité	(Moyen) Un appareil compromis (jailbreaké) permettrait à un attaquant d'avoir un accès complet au système de fichiers, avec accès aux fichiers/instantanés contenant des informations sensibles.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger le brouillage de l'interface utilisateur de l'application mobile [Mis à jour dans Centre de sécurité 1.3]

Configurez la`glide.sg.blur_ui_when_backgrounded` propriété de sorte que l'interface utilisateur de l'application soit floue lorsque l'application est en cours d'exécution en arrière-plan.

Si cette propriété n'est pas définie sur la valeur conseillée **true,** l'interface utilisateur de l'application mobile est visible lorsqu'elle est affichée à partir du commutateur d'application. L'interface utilisateur reste visible même lorsque l'application s'exécute en arrière-plan, ce qui offre un niveau de sécurité et de confidentialité inférieur aux utilisateurs finaux.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sg.blur_ui_when_backgrounded`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 2,4 • Score CVSS : faible • Détails du risque de sécurité : définir la valeur sur **vrai** fournit un niveau plus élevé de confidentialité sur l'appareil local en floutant l'interface utilisateur lorsque l'application est en cours d'exécution en arrière-plan.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Exiger le brouillage de l'interface utilisateur de l'application mobile classique [Mis à jour dans Centre de sécurité 1.3]

Définir la longueur minimale du mot de passe [Mis à jour dans Centre de sécurité 2.2]

Définir une longueur minimale de mot de passe pour éviter les problèmes de conformité et réduire le risque d'une attaque par force brute réussie

Appliquez une longueur minimale de mot de passe d'au moins 12 caractères pour éviter les problèmes de conformité et réduire le risque d'une attaque par force brute réussie.

Pour chaque banque d'informations d'identification de mot de passe utilisée sur votre instance, assurez-vous qu'une politique de mot de passe est appliquée en sélectionnant le champ **Activer la politique de mot de passe** sur l'enregistrement associé dans la table Banque d'informations d'identification de Réinitialisation du mot de passe [pwd_cred_store].

Ensuite, ouvrez l'enregistrement dans la table d'enregistrement Politique de mot de passe [password_policy] et définissez le champ **Longueur minimale du mot de passe** sur **au moins 12**. Vous pouvez trouver l'enregistrement de politique de mot de passe associé dans le champ **Politique de mot de passe** de l'enregistrement Banque d'informations d'identification de réinitialisation du mot de passe [pwd_cred_store].

Pour plus d'informations sur la configuration d'une stratégie de mot de passe, reportez-vous à la section Activer les politiques de mot de passe sur votre instance.

En savoir plus

Attribut	Description
Nom de la configuration technique	Enregistrements des tables Banque d'informations d'identification de réinitialisation du mot de passe [pwd_cred_store] et Politique de mot de passe [password_policy].
Applicabilité du module d'extension	Aucun
Risque de sécurité	Définir la politique de **longueur minimale du mot de passe** [password_policy] enregistrements sur une valeur inférieure à 12 peut entraîner des problèmes de conformité et augmenter le risque qu'un attaquant réussisse à forcer des mots de passe.
Score du système de notation des vulnérabilités courantes (CVSS)	5.9
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	L'instance ne subira aucun impact d'une longueur minimale de mot de passe de 12.
Dépendances et prérequis	Aucun
Type de données	Entier
Valeur de système de base	8
Valeur de secours	8

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	12

Définir la durée de vie de l'OTP pour la réinitialisation du mot de passe à 1 heure [Mis à jour dans Centre de sécurité 2.0]

Contrôlez la durée du lien dans l'e-mail de réinitialisation du mot de passe.

La `glide.pwd_reset.onetime.token.validity` propriété système fait expirer le lien contenu dans l'e-mail de réinitialisation du mot de passe après le nombre d'heures spécifié dans la propriété. La durée de validité d'un jeton de réinitialisation du mot de passe doit être aussi courte que possible sans perturber l'expérience utilisateur normale

Définissez la valeur de la propriété sur 1 (en heures).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.pwd_reset.onetime.token.validity`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1
Valeur par défaut	1
Valeur de secours	1
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,6 • Score CVSS : moyen • Détails du risque de sécurité : une durée de validité plus longue du jeton de réinitialisation du mot de passe donne aux acteurs malveillants une fenêtre plus large pour effectuer la prise de contrôle du compte si l'e-mail contenant le jeton de réinitialisation fait l'objet d'une fuite ou est compromis.
Dépendances et prérequis	Aucun

Logique métier

Cette catégorie examine la logique et le flux propres à chaque application avec des principes généraux de sécurité. Assurez-vous spécifiquement que la séquence prévue de flux de logique métier ne peut pas être contournée, que des limites existent pour détecter et empêcher les attaques automatisées, et que des protections contre les attaques d'usurpation, d'altération, de divulgation d'informations et d'élévation du privilège existent.

Voici quelques-uns des contrôles de sécurité qu'un administrateur peut configurer pour restreindre l'accès non autorisé aux entités sensibles au sein de .ServiceNow AI Platform

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limiter le nombre maximum de commentaires par utilisateur et par jour

Configurez la *sn_kb_social_qa.max_comments_per_user_daily* propriété pour limiter le nombre de commentaires QA par jour.

Si cette propriété n'est pas définie sur la valeur recommandée de **500** ou moins, il n'y a aucune restriction sur le nombre de commentaires QA par jour pouvant entraîner un épuisement des ressources.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_kb_social_qa.max_comments_per_user_daily*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	500
Valeur par défaut	500
Catégorie	Logique métier
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : ne pas définir la valeur recommandée de cette propriété sur 500 ou moins n'impose aucune limite aux commentaires QA par jour, ce qui pourrait entraîner un épuisement des ressources.
Dépendances et prérequis	Aucun

Limiter le nombre maximum d'abonnements par utilisateur et par jour

Configurez la*sn_kb_social_qa.max_subscriptions_per_user_daily* propriété pour limiter le nombre maximal d'abonnements auxquels un utilisateur peut s'abonner par jour.

Si cette propriété n'est pas définie sur la valeur conseillée de **500** ou moins, il n'y a aucune restriction sur le nombre maximal de questions-réponses auxquelles un utilisateur peut s'abonner en une journée. Aucune limitation pourrait entraîner l'épuisement des ressources et avoir un impact sur la disponibilité de votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	500
Valeur par défaut	500

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Logique métier
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : définissez la valeur de la propriété sur 500 ou moins pour éviter l'épuisement des ressources.
Dépendances et prérequis	Aucun

Minimiser la quantité de destinataires SMTP [Mis à jour dans Centre de sécurité 1.3]

Spécifie `glide.email.smtp.max_recipients` le nombre maximal de destinataires que l'instance peut répertorier dans la ligne **À :** pour une seule notification par e-mail.

Défini `glide.email.smtp.max_recipients` sur la valeur recommandée de **100 ou moins**. Les notifications qui dépassent cette limite créent plutôt des notifications par e-mail en double adressées à un sous-ensemble de la liste des destinataires. Chaque notification par e-mail a le même nombre maximum de destinataires.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.smtp.max_recipients`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Logique métier
Objectif	Si cette propriété est définie sur une valeur non sécurisée supérieure à la valeur par défaut de 100, un refus de service peut se produire sur l'instance.
Valeur recommandée	100
Valeur par défaut	100
Type de configuration	Entier
Risque de sécurité	(Modéré) Les notifications qui dépassent cette limite créent plutôt des notifications par e-mail en double adressées à un sous-ensemble de la liste des destinataires.
Cote de risque de sécurité	4.9

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Délai d'expiration des sessions d'invité

Utilisez une propriété système pour contrôler le délai d'expiration de session inactive pour les utilisateurs non authentifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la *glide.guest.session_timeout* propriété système pour définir la durée du délai d'expiration de session inactive (en minutes) pour les utilisateurs non authentifiés. Augmentez la valeur de cette propriété pour prolonger la durée de persistance des sessions de votre instance au-delà de 30 minutes par défaut. Évitez les valeurs de délai d'expiration élevées, qui peuvent augmenter le nombre de sessions conservées par l'instance et causer des problèmes mineurs de disponibilité.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.guest.session_timeout*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Nombre entier (en minutes)
Valeur recommandée	30
Valeur par défaut	30
Valeur de secours	0
Catégorie	Logique métier
Risque de sécurité	• Score de gravité :4.3 • Score CVSS : moyen • Détails du risque de sécurité : des valeurs de délai d'expiration élevées peuvent augmenter le nombre de sessions simultanées sur votre instance, entraînant des problèmes mineurs de disponibilité.
Dépendances et prérequis	Aucun

Valider l'hôte distant

Définissez la propriété sur vrai pour empêcher les acteurs malveillants d'utiliser l'analyse des ports internes sur votre réseau.

Si la *glide.update_set.remote.check_host* propriété n'est pas définie sur la valeur conseillée **true**, la fonctionnalité de test d'instance distante autorise l'analyse des ports internes, une méthode que les acteurs malveillants peuvent utiliser pour découvrir les vulnérabilités d'un réseau. Il est alors possible d'énumérer tous les ports ouverts sur un hôte donné et, dans certains cas, d'extraire les données de réponse qui pourraient entraîner une fuite d'informations ou un accès non autorisé aux données.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.update_set.remote.check_host*
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Logique métier
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails **du risque** de sécurité : ne pas définir la propriété sur la valeur recommandée vrai peut permettre à des acteurs malveillants d'utiliser l'analyse des ports internes pour accéder à des données non autorisées.
Dépendances et prérequis	Aucun
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Define a remote instance

Communications

Ce contrôle garantit un chiffrement approprié à l'aide d'algorithmes et de chiffrements forts. Il s'agit notamment de s'assurer que la version recommandée de TLS est utilisée pour la connectivité client, d'utiliser des suites de chiffrement fortes, d'utiliser des certificats fiables et signés, de s'assurer que les connexions sont chiffrées entre les composants et de consigner les échecs de connexion.

Renforcer l'approbation de certificat [Mis à jour dans Centre de sécurité 1.3, supprimé dans la version 2.0, ajouté dans la version 7.0]

Utilisez les propriétés système pour vous assurer que l'expiration des certificats et la confiance sont vérifiés pour les certificats reçus des points de terminaison d'appels HTTPS sortants lorsque la vérification de l'hôte n'est pas effectuée.

Lorsque `com.glide.communications.trustmanager_trust_all` cette option est définie sur **vrai**, l'expiration du certificat et l'approbation ne sont pas vérifiées pour le certificat reçu d'un point de terminaison d'appel HTTPS sortant lorsque la vérification de l'hôte n'est pas effectuée.

Vérifiez que la `com.glide.communications.trustmanager_trust_all` propriété système est définie sur la valeur conseillée **, faux**. Cela garantit que votre instance ne fait confiance qu'aux certificats qu'elle peut vérifier par rapport au magasin de certificats JVM. Les certificats auto-signés et signés par l'entreprise ne sont pas approuvés. Cette propriété s'applique uniquement lorsque `com.glide.communications.httpclient.verify_hostname` est définie sur **faux**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les valeurs de ces propriétés sont Remplacement sécurisé et ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles). Pour des raisons de sécurité, ne modifiez pas la valeur de cette propriété. Si vous avez d'autres questions, contactez Service client et assistance.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.trustmanager_trust_all`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Communications
Objectif	Pour appliquer la validation de certificat pour les demandes sortantes.
Valeur recommandée	Faux
Cote de risque de sécurité	5.7
Impact fonctionnel	Cette correction applique une validation stricte sur le champ de l'autorité de certification (autorité de certification). Si une entité de confiance (CA) a émis le certificat, l'instance l'accepte pour une utilisation ultérieure.
Risque de sécurité	(Moyen) Pour des raisons de confidentialité et d'intégrité, l'application doit valider l'autorité de certification du certificat avant d'utiliser le certificat pour toute opération transactionnelle.
Références	Certificats Vérifier la chaîne et le nom d'hôte des certificats [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]

Désactiver les connexions SSLv2/SSLv3 sortantes [Mis à jour dans Centre de sécurité 1.3]

Utilisez cette `glide.outbound.sslv3.disabled` propriété pour forcer le Serveur MID à utiliser TLS lors de connexions sortantes, telles que des demandes REST et SOAP. Normalement, les connexions sortantes d'une instance sont forcées d'utiliser TLS au lieu de SSL.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.outbound.sslv3.disabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Communications
Objectif	Pour appliquer l'utilisation de TLS pendant toutes les connexions sortantes à partir de l'instance ServiceNow.
Valeur recommandée	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	Faux **Important :** La valeur de la `glide.outbound.sslv3.disabled` propriété est un remplacement sûr et ne peut pas être modifiée une fois modifiée.
Cote de risque de sécurité	6.5
Impact fonctionnel	Cette correction impose l'utilisation de la version du protocole TLS lors de la communication sur HTTPS. S'il existe des appareils utilisés par les clients/utilisateurs de l'instance qui ne prennent pas en charge la communication TLS, il peut y avoir une panne potentielle.
Risque de sécurité	(Modéré) Les anciennes versions de SSL se sont avérées non sécurisées lorsqu'elles étaient utilisées pour l'implémentation du shell sécurisé HTTP, en raison d'attaques côté client, y compris BEAST et SSL heart-bleed.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

N'utilisez pas de certificats de démonstration pour les configurations SAML actives [Mis à jour dans Centre de sécurité 1.5]

Contrôlez si des certificats de démonstration sont utilisés dans les configurations SAML de production.

Les certificats de démonstration fournis par ServiceNow ne doivent pas être utilisés dans les configurations SAML de production, car ils sont communs à toutes les instances avec une phrase de sécurité connue. Si l'une des propriétés SAML utilisant un magasin de clés de certificat est active (`require_signed_authnrequest`, `require_signed_logoutrequest`ou `encrypt_assertion`), les données de démonstration ne doivent pas être utilisées. Étant donné que les données de démonstration sont partagées entre toutes les instances, il n'existe aucune garantie d'intégrité des demandes signées avec des certificats partagés. Par conséquent, tout message chiffré par l'IDP pourrait être déchiffré par un acteur malveillant s'il était intercepté.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.sso.saml2.keystore`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	sys_id d'un magasin de clés personnalisé
Valeur par défaut	chaîne vide
Catégorie	Communications

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible
Dépendances et prérequis	Aucun

Désactiver les versions TLS déconseillées

Évitez la perte ou la fuite de données sensibles en désactivant les versions TLS déconseillées.

Confirmez que votre instance négocie uniquement la communication via les versions 1.2 de Transport Layer Security (TLS) lorsqu'elle communique avec d'autres serveurs afin d'éviter le transfert de données sur des versions de protocole TLS 1 et TLS 1.1 plus faibles.

Définissez **le fichier com.glide.communications.disable.deprecated.tls** sur **true** pour n'utiliser que les versions TLS 1.2 et ultérieures.

En savoir plus

Attribut	Description
Nom de la configuration technique	com.glide.communications.disable.deprecated.tls
Applicabilité du module d'extension	Aucun
Risque de sécurité	L'utilisation de versions TLS obsolètes et non prises en charge peut entraîner la perte et la fuite de données sensibles.
Score du système de notation des vulnérabilités courantes (CVSS)	4.4
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	Lorsque cette propriété est définie sur **vrai**, les serveurs plus anciens non sécurisés qui nécessitent un protocole TLS 1 ou 1.1 plus faible ne sont pas en mesure de communiquer avec votre instance.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	vrai
Valeur de secours	vrai
Valeur recommandée	vrai

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]

Découvrez comment configurer la propriété pour empêcher les acteurs malveillants de contourner les *com.glide.communications.httpclient.ocsp_allow_network_error* vérifications OCSP (Online Certificate Status Protocol).

Si *com.glide.communications.httpclient.ocsp_allow_network_error* n'est pas défini sur la valeur recommandée faux et que la vérification OCSP (Online Certificate Status Protocol) rencontre une erreur réseau (par exemple, un délai d'expiration ou un problème lors de l'extraction des informations de révocation), elle contourne la vérification de sécurité OCSP et la considère comme réussie. Cela pourrait permettre à un attaquant avec un certificat révoqué de rompre l'infrastructure de clé publique (PKI) et la confiance du certificat numérique qui sont à la base du Web. L'utilisation de certificats révoqués est souvent un indicateur d'activité malveillante, sauf si les serveurs sont désynchronisés.

Assurez-vous que la propriété *com.glide.communications.httpclient.ocsp_allow_network_error* existe et qu'elle est définie sur faux. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.communications.httpclient.ocsp_allow_network_er*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Catégorie	Communications
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur faux peut permettre à un acteur malveillant de contourner le contrôle de sécurité OCSP.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine si une demande relative à l'URI OCSP (Online Certificate Status Protocol) de l'AIA (Authority Information Access) aboutit à une réussite ou à un échec en cas d'erreur de connexion ou de délai d'expiration. Lorsque la valeur est définie sur faux, l'état de révocation du certificat de serveur présenté ne peut pas être validé et entraîne une défaillance de la communication avec ce point de terminaison. Si une erreur réseau se produit lorsque la propriété est définie sur sa valeur par défaut true, le certificat est considéré comme valide du point de vue de la révocation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vérifier la chaîne et le nom d'hôte des certificats [Nouveau dans Security Center 1.3 et mis à jour dans la version 2.0]

Configurez la propriété pour empêcher les *com.glide.communications.httpclient.verify_hostname* attaques de l'intercepteur en veillant à ce que le processus de vérification de certification soit exécuté.

Lorsque la propriété *com.glide.communications.httpclient.verify_hostname* Glide n'est pas définie sur la valeur sécurisée true, le nom d'hôte et la chaîne de certification présentés par les hôtes distants lors d'une connexion TLS initiée à partir de l'instance ServiceNow ne sont pas validés. Cela pourrait compromettre la sécurité de la connexion TLS et permettre des attaques de l'homme du milieu, où les communications entre deux parties sont interceptées. Cela peut entraîner la divulgation de données sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.communications.httpclient.verify_hostname*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Communications
Risque de sécurité	• Score de gravité : élevé • Score CVSS : 7,4 • Détails du risque de sécurité : ne pas définir *com.glide.communications.httpclient.verify_hostname* la valeur recommandée sur vrai peut rendre votre instance vulnérable aux attaques de l'intercepteur du milieu.
Dépendances et prérequis	Aucun
Impact fonctionnel	Vérifie le nom d'hôte et la chaîne de certification présentés par les hôtes SSL (secure socket layer) distants. Définissez cette propriété sur vrai pour vous protéger contre les attaques de l'homme du milieu (MITM). **Remarque :** Cette propriété remplace la *com.glide.communications.trustmanager_trust_all*propriété

Vérifier la révocation du certificat [nouveau dans Security Center 1.3]

La *com.glide.communications.httpclient.verify_revoked_certificate* propriété vérifie la révocation du certificat pendant l'établissement de liaison TLS (Transport Layer Security) pour s'assurer que les contrôles de sécurité ne sont pas contournés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si *com.glide.communications.httpclient.verify_revoked_certificate* la valeur **recommandée n'est** pas définie sur vrai, la révocation du certificat ne sera pas vérifiée pendant l'établissement de liaison TLS. TLS crypte les données envoyées sur Internet pour s'assurer que les acteurs malveillants ne peuvent pas voir les informations sensibles telles que les mots de passe ou les numéros de carte de crédit. Le contournement de la négociation TLS constitue un risque pour la sécurité, car un attaquant dont le certificat a été révoqué peut négliger de fournir un certificat valide et rompre l'infrastructure à clé publique (PKI) et la confiance dans le certificat numérique.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.communications.httpclient.verify_revoked_certif*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Communications
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si la valeur *com.glide.communications.httpclient.verify_revoked_cert* recommandée est true, la révocation du certificat ne sera pas vérifiée pendant l'établissement de liaison TLS.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété doit être définie sur vrai pour s'assurer qu'une session TLS (Transport Layer Security) est démarrée avec un point de terminaison authentique. Si cette propriété est définie sur faux, le certificat n'est pas vérifié, ce qui peut compromettre la sécurité de l'instance.

Traduction automatique

Configuration

La catégorie Configuration garantit que les applications disposent d'un environnement de build sécurisé et de composants de bibliothèque tiers renforcés. Plus précisément, il s'agit de s'assurer qu'un pipeline de création et de déploiement est répétable et inclut des tests automatisés, et empêche le déploiement des problèmes de sécurité connus. Cela inclut la mise à jour des dépendances et l'absence de vulnérabilités connues.

Options de type de contenu de définition automatique [supprimé dans Centre de sécurité 1.3.3]

Configurez la propriété Options de type de contenu défini automatiquement sur votre instance pour éviter les attaques de confusion MIME.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez cette propriété pour contrôler l'en-tête HTTP de réponse X-Content-Type-Options. L'en-tête HTTP de réponse X-Content-Type-Options est utilisé par le serveur pour indiquer que les types MIME publiés dans les en-têtes Content-Type doivent être suivis. Si cette propriété est définie sur faux, il est possible qu'un attaquant mène des attaques de confusion MIME ; Sila valeur est true , cet en-tête empêchera le navigateur d'interpréter les fichiers comme autre chose que le type de contenu dans les en-têtes HTTP.

⚠ Avertissement :
La valeur de cette propriété est un remplacement sans base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.header.auto_set_x_content_type_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	Faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 7,3 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **faux** pourrait permettre à un attaquant de mener des attaques de confusion MIME.
Dépendances et prérequis	Aucun
Références	Add a system property

Valeur d'en-tête HTTP de contrôle de cache [mise à jour dans Centre de sécurité 1.3 et supprimée dans 1.5]

Utilisez la `glide.http.cache_control` propriété pour définir la valeur de contrôle de cache par défaut dans les en-têtes de réponse HTTP envoyés lors de la ServiceNow AI Platform demande de données de contenu statique pour une page. Les exemples de contenu statique incluent les images, le CSS et le JavaScript rendus de l'intérieur, pour une page.

La `glide.http.cache_control` propriété définit la valeur de contrôle de cache par défaut dans les en-têtes de réponse HTTP sur **privé** ou **public**. La valeur par défaut est **privée**.

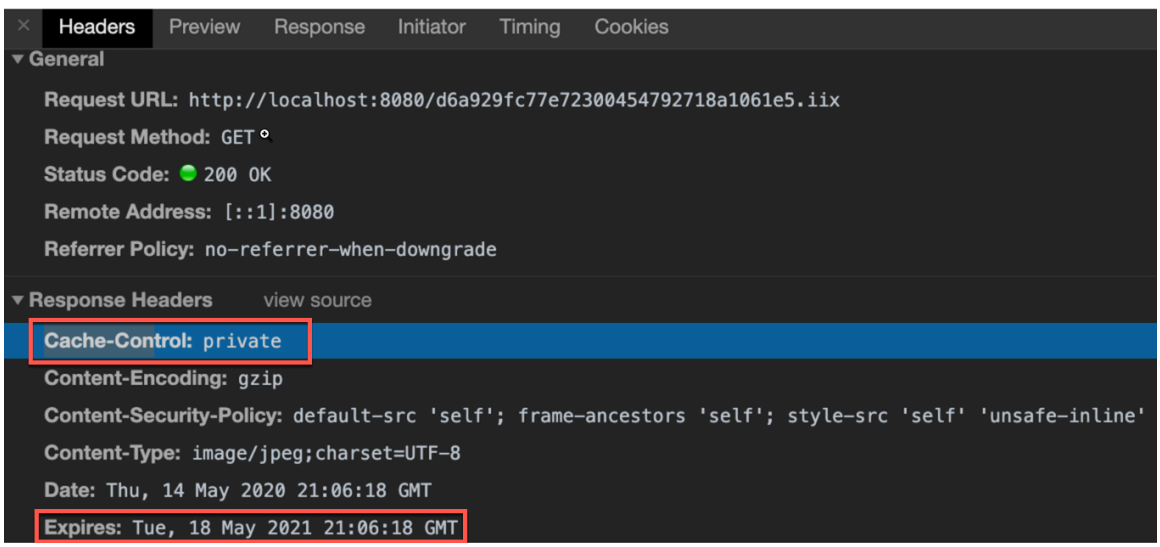
Valeur	Description
privé	Le contenu statique peut être mis en cache au niveau du navigateur (client), mais pas au niveau du serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur	Description
publique	Le contenu statique peut être mis en cache au niveau du navigateur (client), ainsi qu'au niveau du serveur proxy.

La valeur Expire dans les en-têtes de réponse HTTP contrôle le moment où le contenu statique expire et a une valeur par défaut de 369 jours. Pour remplacer manuellement la valeur par défaut, utilisez la `glide.http.expire.days` propriété.



Remarque :
Vous pouvez utiliser la propriété pour indiquer s'il `glide.http.cache` faut activer ou désactiver le paramètre des valeurs Cache-Control et Expires dans les en-têtes de réponse HTTP. Sa valeur par défaut est **true**, ce qui vous permet de définir les éléments suivants :

- Valeur de contrôle de cache par défaut utilisant la `glide.http.cache_control` propriété.
- Fait expirer la valeur par défaut à l'aide de la `glide.http.expire.days` propriété.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.http.cache_control`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Pour configurer la valeur d'en-tête de réponse HTTP de contrôle de cache pour le contenu statique.
Valeur recommandée	privé
Valeur par défaut	privé
Cote de risque de sécurité	4.3
Impact fonctionnel	Définit la valeur de contrôle de cache par défaut dans un en-tête de réponse HTTP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Si vous définissez cette propriété sur **public**, les instances avec CDN/proxys peuvent mettre en cache le contenu statique et s'afficher sans authentification. • **privé** est un paramètre plus approprié pour les instances avec configuration CDN/proxy. • Si l'instance ne dispose pas d'une configuration CDN/proxy, l'une ou l'autre valeur devrait convenir.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la configuration des en-têtes de réponse HTTP

Réduisez le risque de détournement de cookies/de session des applications Web à l'aide d'une propriété système.

Si *glide.http.headers_config.enabled* la valeur n'est pas définie sur **vrai**, les configurations d'en-tête de réponse définies dans la table En-têtes de réponse HTTP [sys_response_header] ne sont pas utilisées. Les en-têtes de réponse HTTP liés à la sécurité incluent la politique de sécurité du contenu, qui contribue aux protections liées aux XSS. Pour plus d'informations sur les en-têtes de réponse HTTP, reportez-vous à la section HTTP Response Headers .

Vérifiez que la propriété *glide.http.headers_config.enabled* est définie sur **true**.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.http.headers_config.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Valeur de secours	vrai
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 5,5 • Score CVSS : moyen • Risque de sécurité : les risques de sécurité d'en-têtes de réponse HTTP manquants, incorrects ou faibles peuvent permettre le détournement XSS, CSRF et lié aux cookies/sessions des applications Web.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le débogage du serveur de messagerie instantanée

Activez ou désactivez les journaux système de votre instance en configurant cette propriété.

Utilisez cette propriété pour gérer la façon dont votre instance gère les`glide.cs.debug`journaux système. Si la propriété est définie sur la valeur recommandée **faux**, les journaux système ne sont pas activés. Si la valeur est définie sur **vrai**, les journaux système sont activés. Définissez la propriété sur **vrai** uniquement lorsque vous souhaitez dépanner, puis désactivez-la lorsque vous avez terminé. L'activation des journaux système peut entraîner la génération de nombreux messages, ce qui peut surcharger les journaux système. Les messages du journal peuvent exposer par inadvertance des informations sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.cs.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 2,3 • Score CVSS : faible • Détails du risque de sécurité : l'activation des journaux système peut entraîner la génération de nombreux messages susceptibles de surcharger le système de messages de journal exposant par inadvertance des informations sensibles.
Dépendances et prérequis	Aucun

Désactiver l'utilisation de l'interface utilisateur JQuery héritée

Évitez l'introduction de vulnérabilités non corrigées dans la bibliothèque en désactivant l'utilisation de l'interface utilisateur JQuery héritée.

Empêchez l'utilisation d'anciennes versions d'interface utilisateur jQuery prédéfinies, qui introduisent des vulnérabilités non corrigées dans la bibliothèque. L'utilisation d'anciennes versions peut potentiellement entraîner des risques de sécurité découlant des attaques sur les vulnérabilités détectées dans les versions obsolètes de la bibliothèque d'interface utilisateur JQuery.

Confirmez que la propriété système **glide.jquery_ui.legacy** est définie sur **false** pour empêcher l'utilisation d'anciennes versions d'interface utilisateur jQuery prédéfinies. Cette propriété système est une sécurité au cas où les organisations dépendent des versions non corrigées pour exécuter leurs implémentations personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.jquery_ui.legacy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Valeur de secours	vrai
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible • Empêcher l'utilisation d'anciennes versions d'interface utilisateur jQuery prédéfinies peut introduire des vulnérabilités non corrigées dans la bibliothèque.
Impact fonctionnel	Cette propriété système est une sécurité au cas où les organisations dépendent des versions non corrigées pour exécuter leurs implémentations personnalisées.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver le débogage des éléments de formulaire verrouillés

Voici la description pour `glide.security.explain.write.locks`.

Définissez `glide.security.explain.write.locks` la valeur recommandée sur **faux** pour empêcher l'affichage d'une explication des éléments de formulaire verrouillés. Définissez la valeur sur **vrai** pour afficher l'explication des éléments de formulaire verrouillés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.explain.write.locks`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Limite le comportement d'affichage de SecurityDebugger sans dépendance à d'autres propriétés.
Valeur recommandée	Faux
Valeur par défaut	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Booléen
Risque de sécurité	(Faible) Empêchera l'affichage de l'explication sur les éléments de formulaire verrouillés. Cela rend l'application légèrement plus sécurisée, car moins d'informations sont fournies par le débogueur de sécurité.
Cote de risque de sécurité	3,5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver le débogage MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]

La `glide.authenticate.multisso.debug` propriété contrôle la journalisation des débogages pour Multi-SSO.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multisso.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Désactive le débogage SSO de plusieurs fournisseurs.
Valeur recommandée	Faux
Valeur par défaut	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Définissez la propriété sur la valeur recommandée « Faux », sinon, le débogage MultiSSO est activé, ce qui pourrait entraîner une fuite d'informations sensibles involontaire.
Cote de risque de sécurité	4
Références	Propriétés, tables et scripts SSO de plusieurs fournisseurs

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Interdire le clonage cible [Nouveau dans Security Center 1.3]

Configurez la propriété pour empêcher votre `glide.db.clone.allow_clone_target` instance d'être utilisée comme cible de clone.

Protégez votre instance contre toute utilisation en tant que cible de clone en définissant la propriété système **glide.db.clone.allow_clone_target** sur **false**. Un clone système copie tout ce qui se trouve dans une base de données à partir d'une instance source vers l'instance cible. Il s'agit d'un risque de sécurité, car la base de données d'instance de l'instance cible est écrasée lors du processus de clonage, ce qui entraîne une perte de données et un manque d'intégrité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez la propriété système **glide.db.clone.allow_clone_target** sur **faux sur les** instances de production pour interdire la sélection de votre instance en tant que cible de clone.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.db.clone.allow_clone_target`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée faux permet à l'instance d'être utilisée comme cible du clone. Il s'agit d'un risque pour la sécurité, car la base de données d'instance peut être écrasée lors du processus de clonage.
Dépendances et prérequis	Aucun
Références	• • Register target instance (legacy)
Impact fonctionnel	Cette propriété fournit une protection supplémentaire qui empêche le clonage d'une instance de production. La valeur par défaut est faux pour les instances de production et vrai pour les instances de sous-production telles que dev ou qa. Pour permettre à une instance d'être utilisée comme cible du clone, définissez cette propriété sur vrai.

Désactiver l'affichage de la trace de la pile d'erreurs SOAP

Gérez la façon dont les traces de la pile sont affichées dans votre instance.

Utilisez la propriété pour gérer les `glide.soapfault.display_stack_trace`traces de pile dans votre instance. Si cette propriété est configurée sur **faux**, des informations sensibles risquent d'être divulguées. Si la valeur est définie sur **vrai**, aucune trace de la pile ne s'affichera.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.soapfault.display_stack_trace`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **faux** peut exposer des informations sensibles à partir de la trace de pile.
Dépendances et prérequis	Aucun

Restreindre l'accès à la surveillance des performances [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour contrôler l'accès `glide.security.diag_txns_acl` aux stats.do, threads.do thread_pool_stats et replication.do à partir d'une connexion non authentifiée.

Lorsque vous définissez cette propriété sur **vrai**, elle `glide.security.diag_txns_acl` autorise uniquement l'accès aux éléments suivants par le compte administrateur :

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Sans activer ce paramètre, il est toujours possible d'accéder à ces ressources à partir d'une connexion non authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.diag_txns_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Limiter l'accès aux pages de configuration au compte administrateur uniquement
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	5.3

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	Cette correction applique uniquement le compte administrateur pour accéder aux données sensibles de l'application à des fins de connexion et de dépannage.
Risque de sécurité	(Modéré) Les données sensibles telles que les détails du serveur, les threads et les processus exécutés sur le serveur ne doivent jamais être visibles ou accessibles à l'utilisateur final sans privilèges appropriés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Centre de sécurité 1.3 et 1.5]

Vérifiez que vous utilisez la version 2 du module d'extension MultiSSO et qu'elle est définie sur vrai pour réduire les vulnérabilités de sécurité.

Si le module d'extension Multi SSO est activé sur une instance, réduisez les vulnérabilités de sécurité en confirmant que la version v2 est activée. La dernière version renforce la sécurité et dispose de plus de fonctionnalités, telles que la prise en charge du chiffrement d'assertion et la déconnexion unique (SLO) initiée par IdP. Si la dernière version n'est pas activée, les nouvelles fonctionnalités de sécurité ne peuvent pas être utilisées et l'instance risque d'utiliser un module d'extension déconseillé.

Suivez les étapes de KB0756504 pour effectuer une mise à niveau vers la dernière version. Ce processus comprend la vérification et la migration de tous les changements liés à la personnalisation, puis la mise à niveau de la version. Lorsque vous avez terminé, la propriété système **glide.authenticate.multissov2_feature.enabled** est automatiquement définie **sur vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	glide.authenticate.multissov2_feature.activé
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Configuration
Risque de sécurité	Si la dernière version n'est pas activée, les nouvelles fonctionnalités de sécurité ne peuvent pas être utilisées et l'instance risque d'utiliser un module d'extension déconseillé
Dépendances et prérequis	Aucun
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer la politique de référent sécurisé [Nouveau dans Security Center 1.3]

Utilisez la *com.glide.security.referrerpolicy* propriété pour vous assurer que l'en-tête HTTP Referrer-Policy envoie le niveau de données approprié à chaque ServiceNow® page afin d'éviter les fuites de données.

Lorsque la propriété est définie sur la *com.glide.security.referrerpolicy* valeur par défaut, elle s'assure que l'en-tête HTTP Referrer-Policy est géré avec le niveau approprié d'informations envoyées, spécifiquement adaptées à la ServiceNow AI Platform® page de demande. Cela empêche les fuites de données non autorisées qui pourraient être accessibles à partir d'autres parties de l'URL complète, telles que le chemin d'accès et la chaîne de requête.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.security.referrerpolicy*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	Par défaut
Valeur par défaut	Par défaut
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : assurez-vous que la propriété est définie sur la *com.glide.security.referrerpolicy* valeur par défaut pour éviter les fuites de données non autorisées.
Dépendances et prérequis	Aucun
Références	Politique du référent
Impact fonctionnel	Cette propriété contrôle la quantité d'informations envoyées via l'en-tête de référent lorsqu'une demande est envoyée à partir d'une page : • par défaut : l'instance prend en charge les en-têtes de référent • same-origin : envoyer l'URL référente complète au sein de l'instance/du même domaine et aucun référent vers l'origine extérieure • origin : Envoyer uniquement l'origine en tant que référent à l'intérieur et à l'extérieur de l'origine • origin-when-cross-origin : envoyer l'URL référente complète au sein de l'instance/du même domaine et uniquement l'origine à l'extérieur de l'origine

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Garantir la taille minimale de la clé privée

Utilisez une propriété système pour déterminer la taille minimale de la clé privée utilisée pour la génération de la demande de signature de certificat (CSR) avec l'application Gestion d'inventaire des certificats.

La *sn_disco_certmgmt.private_key_size* propriété système détermine la taille minimale de la clé privée utilisée pour la génération de CSR avec l'application Gestion d'inventaire des certificats. Choix valides : 512, 1024, 2048 ou 4096.

Vérifiez que cette propriété est définie sur une valeur supérieure ou égale à 2 048. Les choix valides pour cette propriété sont 512, 1024, 2048 ou 4096. Si la propriété n'existe pas dans la table Propriétés système [sys_properties], ou si la valeur n'est pas valide, la valeur est 2048 par défaut.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_disco_certmgmt.private_key_size*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Nombre entier représentant la taille de la clé privée générée. Utilisez des valeurs de 512, 1024, 2048 ou 4096.
Valeur recommandée	2048
Valeur par défaut	2048
Valeur de secours	2048
Catégorie	Communications
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Risque de sécurité : l'utilisation de clés antérieures à 2048 peut entraîner la divulgation d'informations futures en cas de force brute de la clé. Utilisez une valeur valide supérieure ou égale à 2 048 pour assurer la pérennité de la clé sur une période plus longue.
Impact fonctionnel	Les systèmes et applications hérités ne peuvent pas gérer de clés supérieures ou égales à 2048.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mis à jour dans Centre de sécurité 1.3]

Utilisez la *glide.set_x_frame_options* propriété pour définir l'en-tête de réponse X-Frame-Options sur SAMEORIGIN pour toutes les pages de l'interface utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez l'en-tête de réponse HTTP X-Frame-Options pour indiquer si le navigateur doit être autorisé à afficher une page dans un ou <iframe>un <frame> . Les sites peuvent utiliser cette fonction pour éviter les attaques de détournement de clic, en s'assurant que leur contenu n'est pas intégré à d'autres sites. Un attaquant pourrait intégrer votre page dans sa propre page et faire en sorte que les éléments de votre page fonctionnent de manière malveillante. L'utilisateur final peut penser que la page est légitime parce qu'elle ressemble à votre page. L'utilisateur final peut cliquer sur des éléments comme d'habitude pour exécuter des scripts ou des éléments malveillants.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.set_x_frame_options*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Pour atténuer les attaques de ClickJacking.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	5.9
Impact fonctionnel	Cette correction applique la restriction pour le rendu d'une ServiceNow AI Platform application dans une application tierce sous la forme d'un iFrame. Si vous disposez d'une telle intégration, l'application ne s'affichera pas dans l'application tierce personnalisée.
Risque de sécurité	(Moyen) La stratégie de même origine vous permet d'empêcher un domaine de récupérer un script ou une ressource d'un autre domaine. Tous les navigateurs modernes prennent en charge cette fonctionnalité. La politique valide la connexion en fonction du protocole, du port et de l'hôte. CORS (Cross Origin Request) est une modification de la politique de même origine qui permet d'accéder aux ressources/scripts d'un autre domaine lorsqu'elle est explicitement indiquée comme faisant partie de la valeur d'en-tête. • Dans ce cas, l'en-tête X-Frame-Options contrôle si l'application ServiceNow AI Platform peut être affichée sur le site Web tiers. • Cela réduit l'exposition sensible, car la valeur de propriété, lorsqu'elle est définie sur **SAMEORIGIN** , ne permet pas le rendu de se produire.
Références	Propriétés système disponibles Configurer les iFrame

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exiger un accès en écriture pour accéder à la page Ajouter un élément du catalogue de services [Nouveau dans Security Center 1.3]

Utilisez la propriété pour empêcher l'exécution `glide.sc.request.add_item_write_access` d'opérations non autorisées sur les éléments de catalogue.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sc.request.add_item_write_access`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : lorsque la `glide.sc.request.add_item_write_access` propriété est définie sur faux, tout utilisateur connecté peut accéder à la page de l'interface utilisateur Ajouter un élément de catalogue. Cela peut entraîner la réalisation d'opérations non autorisées sur les éléments de catalogue. Pour remédier à ce risque de sécurité, définissez cette propriété sur vrai.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque la propriété est définie sur vrai, l'utilisateur doit avoir un accès en écriture à l'enregistrement dans le contexte de la page de l'interface utilisateur.

Définir des options XFrame pour empêcher l'intégration de sites Web tiers [Mis à jour dans Centre de sécurité 1.3]

Configurez cette propriété pour empêcher l'intégration du contenu d'une application Web dans un site tiers.

Si `com.glide.cs.embed.xframe_options` n'est pas défini sur la valeur recommandée DENY ou SAMEORIGIN, le contenu de l'application Web peut être incorporé dans un site tiers à l'aide d'un URI ALLOW-FROM. Autoriser des sites tiers non approuvés pourrait permettre des attaques telles que le détournement de clic.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.cs.embed.xframe_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	Sameorigin
Valeur par défaut	Sameorigin
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur la valeur recommandée, il est possible d'intégrer le contenu d'une application Web dans un site tiers, ce qui permet des attaques telles que le click-jacking.
Dépendances et prérequis	Aucun

Protection des données

La catégorie de protection des données traite des éléments de confidentialité, d'intégrité et de disponibilité (CIA) des données.

Les composantes CIA sont les suivantes :

- Confidentialité : les données sont protégées contre tout accès non autorisé en transit et au repos.
- Intégrité : les données sont protégées contre toute création, suppression ou modification non autorisée.
- Disponibilité : les données sont accessibles au besoin.

Supprimer Se souvenir de moi

Utilisez la `glide.ui.forgetme` propriété pour supprimer la case **à cocher « Se souvenir de moi** » de la page de connexion afin d'éviter que les informations de connexion ne soient mises en cache.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.forgetme`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Protection des données

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour garantir qu'aucune information d'authentification n'est mise en cache.
Cote de risque de sécurité	3,5
Valeur recommandée	vrai
Valeur par défaut	vrai
Impact fonctionnel	Cette correction changerait l'expérience utilisateur en le déconnectant automatiquement de l'instance à l'expiration de sa session. L'expiration de la session dépend uniquement de la valeur définie dans la propriété système, comme détaillé dans Managing user sessions .
Risque de sécurité	(Faible) Lorsque vous cochez la case **Se souvenir de moi** lors de la connexion, un cookie supplémentaire est stocké sur l'ordinateur de l'utilisateur. • Son but est de rétablir automatiquement la session pour les visites ultérieures de l'utilisateur connecté. • Il présente un risque de sécurité car il permet à la session utilisateur d'être active jusqu'à ce qu'il se déconnecte délibérément. La probabilité d'une attaque dans ce scénario augmente lorsque l'utilisateur final a laissé le navigateur sans surveillance ou s'il est compromis par une autre attaque.
Références	Supprimer la case à cocher Se souvenir de moi

Pour en savoir plus sur l'ajout ou la création d'une propriété système, voir Add a system property

Exiger l'effacement du presse-papiers lors de l'affichage l'application mobile en arrière-plan [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La *glide.sg.clear_pasteboard_when_backgrounded* propriété contrôle si le texte copié à partir de l'application mobile ServiceNow est conservé dans le presse-papiers une fois que l'application est en mode arrière-plan. Si elle n'est pas définie sur la valeur conseillée true, les informations sensibles peuvent être divulguées au presse-papiers Android ou iOS, où elles peuvent être exposées à d'autres applications sur l'appareil.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.sg.clear_pasteboard_when_backgrounded*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée vrai, les informations sensibles peuvent être divulguées au presse-papiers Android ou iOS, où elles peuvent être exposées à d'autres applications sur l'appareil.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété efface le copier/coller du presse-papiers lorsque l'application ServiceNow passe en arrière-plan.

Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Utilisez cette`sn_hr_core.restrict_guest_email` propriété afin de contrôler si un utilisateur peut répondre à un ticket RH avec son adresse e-mail personnelle.

Lorsque la `sn_hr_core.restrict_guest_email` propriété n'est pas définie sur vrai, un utilisateur peut envoyer un e-mail à partir d'un compte personnel en référence au ticket RH à inclure dans les notes de travail. Cela peut entraîner des problèmes mineurs de confidentialité ou d'intégrité si l'e-mail personnel est compromis ou si la communication n'est pas sécurisée. Un administrateur peut vouloir restreindre la capacité des utilisateurs à répondre aux tickets RH à partir de leur adresse e-mail personnelle, car il ne peut pas être sûr de l'identité de l'utilisateur qui accède au compte de messagerie personnel.

En savoir plus

Attribut	Description
Nom de la configuration	`sn_hr_core.restrict_guest_email`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	Faux
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : le fait que cette propriété ne soit pas définie sur vrai peut entraîner des problèmes mineurs de confidentialité ou d'intégrité si l'e-mail personnel est compromis ou si la communication n'est pas sécurisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété contrôle si une réponse provenant d'une adresse e-mail personnelle met à jour ou non un ticket RH. Si la valeur est définie sur vrai, toute réponse provenant d'un e-mail personnel sera ajoutée aux notes du ticket. Si la valeur est faux, le ticket et les notes ne seront pas mis à jour.

Restreindre les paramètres OAuth au corps POST [nouveau dans Security Center 1.3]

Utilisez la `glide.oauth.allow.parameters.in.post.body.only` propriété pour contrôler l'acceptation des jetons d'accès par l'authentification OAuth entrante. Les jetons d'accès sont sensibles et ne doivent être acceptés que lorsqu'ils se trouvent dans le corps d'une demande POST.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.oauth.allow.parameters.in.post.body.only`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : si `glide.oauth.allow.parameters.in.post.body.only` n'est pas défini sur la valeur recommandée **vrai**, des jetons d'accès peuvent être présents dans le paramètre de demande GET. Ces jetons d'accès pourraient persister dans les journaux des clients et de l'infrastructure et potentiellement conduire à la prise de contrôle des comptes en cas de fuite de ces journaux.
Dépendances et prérequis	Aucun
Références	• OAuth 2.0 • Gérer les jetons OAuth
Impact fonctionnel	Garantit que le processeur oauth_token.do accepte uniquement les paramètres de corps POST comme entrée pour tous les types d'accord pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion et journalisation des erreurs

La catégorie Gestion des erreurs et journalisation traite de la qualité et de la verbosité des informations journalisées exposées aux personnes concernées.

Il s'agit notamment de s'assurer que les journaux et les messages d'erreur ne collectent pas d'informations sensibles, protègent correctement les données conformément à la classification et ont une durée de vie appropriée. En outre, cette catégorie concerne le traitement approprié des erreurs et le fait de ne pas révéler les erreurs sensibles aux utilisateurs finaux, telles que les traces de pile verbeuses pour les exceptions non gérées ayant des implications en matière de sécurité.

Désactiver l'enregistreur pour les utilisateurs avec faibles privilèges dans le bac à sable de script [Mis à jour dans Centre de sécurité 1.3]

Gérez la capacité du système Glide à consigner les scripts en cours d'exécution dans l'environnement sandbox.

Utilisez cette propriété pour contrôler la `glide.security.sandbox_no_logging` capacité du système Glide à consigner les scripts en cours d'exécution dans l'environnement sandbox. Si `glide.security.sandbox_no_logging` la valeur est définie sur **faux**, la journalisation est disponible pour les utilisateurs ayant des privilèges inférieurs à l'aide de scripts bac à sable. Il s'agit d'une faille de sécurité potentielle, car les utilisateurs ayant peu de privilèges peuvent injecter des journaux, ce qui permet à un acteur malveillant d'obfusquer une attaque. Configurez la propriété sur **vrai** pour empêcher les utilisateurs avec des privilèges inférieurs qui utilisent un script bac à sable d'avoir une fonctionnalité de journalisation.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.sandbox_no_logging`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 2,2 • Score CVSS : faible • Détails du risque de sécurité : définir cette propriété sur **faux** permet la connexion pour les utilisateurs ayant moins de privilèges, ce qui pourrait permettre à un acteur malveillant de masquer une attaque.
Dépendances et prérequis	Aucun

Désactiver le débogage des cookies sécurisés

Gérez les messages de journal associés aux cookies dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la propriété pour gérer vos`glide.secure_cookie.debug` messages de journal liés aux cookies. Si cette propriété est définie sur **faux**, aucun message du journal n'est affiché. Si elle est définie sur **true**, les messages des classes `SecureUserCookie` et `Cookie` sont journalisés. Cela peut entraîner l'exposition d'informations sensibles dans votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.secure_cookie.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : la configuration de cette propriété sur **vrai** peut entraîner l'exposition d'informations sensibles.
Dépendances et prérequis	Aucun

Désactiver les messages d'erreur SQL [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez cette propriété pour désactiver l'affichage `glide.db.loguser` des messages d'erreur SQL dans un navigateur.

Si `glide.db.loguser` cette option n'est pas définie sur la valeur conseillée, faux, des messages d'erreur sensibles côté serveur peuvent être affichés aux utilisateurs finaux. Les messages d'erreur peuvent inclure des traces de pile et des informations sur la structure de la base de données qui pourraient fournir à un attaquant les connaissances nécessaires pour effectuer une injection SQL réussie si les conditions préalables sont réunies. Dans le cadre d'une défense en profondeur, ces messages d'erreur ne doivent pas être affichés à l'utilisateur final.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.db.loguser`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion et journalisation des erreurs
Objectif	Pour désactiver l'affichage des messages d'erreur SQL dans le navigateur.
Type	Booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	Faux
Valeur par défaut	vrai
Cote de risque de sécurité	3.1
Impact fonctionnel	Cette correction désactive le rendu des messages d'erreur SQL. Il n'y a aucun impact sur les fonctionnalités.
Risque de sécurité	(Moyen) Aucune information SQL sensible susceptible d'aider un attaquant ne doit apparaître dans le message d'erreur d'une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le journal d'audit MID [nouveau dans Security Center 1.3 et mis à jour dans 1.5]

Le journal d'audit des commandes de Serveur MID enregistre des détails tels que le nom de la commande, le hachage de la commande, le nom des informations d'identification utilisées et l'état d'exécution.

Une fois activés, les journaux d'audit peuvent être consultés par les utilisateurs ayant le rôle agent_security_admin dans la table ecc_agent_command_audit_log ou en accédant à **Serveur MID** > **Journaux d'audit de commande**.

Définissez `mid.log.command_audit.enable` la valeur sur vrai dans la table Propriétés du Serveur MID [ecc_agent_property] pour activer l'audit des commandes exécutées par le Serveur MID.

En savoir plus

Attribut	Description
Nom de la configuration	`mid.log.command_audit.enable`
Type de configuration	Enregistrement de la propriété de Serveur MID [ecc_agent_property]
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 2,2 • Score CVSS : faible • Détails du risque de sécurité : en cas d'examen de sécurité, cette table peut être utilisée par les équipes de réponse aux incidents pour auditer les commandes exécutées sur le Serveur MID. Sans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	ce journal, il n'y aurait peut-être pas suffisamment de détails pour répondre à des situations telles que l'utilisation non autorisée d'un compte.
Dépendances et prérequis	Aucun

Activer le module d'extension Tables protégées [nouveau dans le centre de sécurité 1.3]

Utilisez la propriété pour empêcher les `com.glide.security.protected_table.enabled` utilisateurs avec des privilèges plus élevés d'altérer les tables de journal.

Lorsque la propriété est définie sur **vrai**, le `com.glide.security.protected_table.enabled` module d'extension Tables protégées est utilisé pour empêcher les utilisateurs avec des privilèges plus élevés sur une instance d'altérer les tables de journal. Les tables de journal suivantes bénéficient de protections spéciales lorsque cette propriété est définie sur **vrai** :

- syslog (aucun remplacement de base de données)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- protected_table_configuration (aucun remplacement de base de données)

L'intégrité des journaux est importante pour déterminer l'activité malveillante sur une instance par un administrateur client.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.security.protected_table.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 4,5 • Score CVSS : moyen • Détails du risque de sécurité : le fait de ne pas définir `com.glide.security.protected_table.enabled`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	la valeur recommandée sur vrai permet aux utilisateurs avec des privilèges plus élevés sur une instance d'altérer les tables de journal.
Dépendances et prérequis	Aucun
Références	Journaux système

Consigner tous les champs de demande HTTP sortants [Supprimé dans Centre de sécurité v1.3.2]

Configurez lapropriété sur false pour empêcher les *glide.outbound_http.security.log.allow.all.fields* champs HTTP sortants sensibles d'être consignés en texte brut.

Si cette propriété n'est pas définie sur la valeur recommandée **faux**, les champs HTTP sortants sensibles peuvent être consignés en texte brut. Cela peut réduire la posture de sécurité de votre réseau d'entreprise, car les demandes sortantes contenant des données et des informations d'identification sensibles peuvent être enregistrées en texte brut non chiffré et peuvent être consultées par les utilisateurs ayant moins de privilèges.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.outbound_http.security.log.allow.all.fields*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	30
Valeur par défaut	30
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 6,8 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur **faux** augmente le risque que des champs sortants sensibles soient consignés en texte brut, ce qui constitue un risque pour la sécurité.
Dépendances et prérequis	Aucun

Nettoyage HTML du journal [supprimé dans Centre de sécurité 2.0]

Configurez *glide.html_sanitize.discarded_log.enable* la propriété permettant de déterminer si les événements de nettoyage HTML sont journalisés dans votre instance.

Si cette propriété n'est pas définie sur la valeur recommandée **vrai**, les événements de nettoyage HTML ne sont pas consignés dans la *sys_log* table. L'absence de journalisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

peut avoir un impact négatif sur les options automatisées de détection et d'investigation de sécurité de votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.html_sanitize.discarded_log.enable`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 2,4 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée **vrai**, les événements d'assainissement HTML ne sont pas consignés dans la table, ce qui peut avoir un impact sur les `sys_log` options automatisées de détection et d'enquête de sécurité.
Dépendances et prérequis	Aucun
Références	Activation de l'assainisseur HTML

Consigner les événements d'audit de session [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Définissez la propriété sur **vrai** pour que les `glide.authenticate.session_access.log_audit_event` événements d'audit de session soient créés dans la `sys_session_access_audit` table.

Lorsque la propriété `glide.authenticate.session_access.log_audit_event` Glide est définie sur vrai, les événements d'audit de session sont créés dans la table sys_session_access_audit. Il est recommandé de consigner des informations sur l'accès à une session pour faciliter les enquêtes sur les acteurs malveillants. Les informations enregistrées comprennent l'utilisateur, l'ID de session (non sensible), l'adresse IP, les rôles et les politiques.

Remarque :
La `glide.authenticate.session_access.log_audit_event` propriété système est spécifique à l'accès Zero Trust. Pour plus d'informations, consultez Accès zéro confiance (ZTA).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.log_audit_event`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : le fait de ne pas définir cette propriété sur la valeur recommandée vrai empêche la journalisation des événements. Cela pourrait vous empêcher de trouver des acteurs malveillants en cas de cyberattaque.
Dépendances et prérequis	Aucun

Enregistrer l'emprunt d'identité d'un utilisateur [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Configurez `glide.sys.log_impersonation` pour contrôler si des événements d'emprunt d'identité de l'utilisateur sont consignés dans votre instance.

Si cette propriété **n'est** pas définie sur la valeur recommandée vrai, les événements d'emprunt d'identité de l'utilisateur ne sont plus consignés. L'absence de journalisation peut avoir un impact sur les options automatisées de détection et d'investigation de sécurité de votre instance. Assurez-vous que la propriété `glide.sys.log_impersonation` existe et qu'elle est définie sur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sys.log_impersonation`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	VRAI
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur **vrai**, les événements d'emprunt d'identité de l'utilisateur ne sont plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	consignés, ce qui pourrait avoir un impact sur les options de détection et d'investigation de sécurité de votre instance.
Dépendances et prérequis	Aucun
Références	Impersonating users

Empêcher la journalisation des requêtes HTTP détaillées

Empêcher l'accès aux informations sensibles en réduisant la journalisation des requêtes HTTP détaillées.

Contrôlez le niveau de journalisation des demandes HTTP sortantes afin d'empêcher l'accès à des informations sensibles, telles que les en-têtes d'autorisation ou les cookies. Ces informations peuvent être utilisées comme des informations d'identification pour accéder à la ressource demandée.

Le niveau de journalisation de ces demandes est contrôlé par les propriétés **glide.outbound_http_log.override** et **glide.outbound_http_log.override.level** . Lorsque **glide.outbound_http_log.override** est défini sur **vrai**, le niveau de journalisation des demandes et des réponses est contrôlé par la propriété **glide.outbound_http_log.override.level** . Si **glide.outbound_http_log.override.level** est défini sur **tous** ou **élevé**, les en-têtes de demande et de réponse sont journalisés.

Définissez **glide.outbound_http_log.override** sur **faux** et **glide.outbound_http_log.override.level** sur **basique**. Si ces propriétés n'apparaissent pas dans la table Propriétés système [sys_properties], elles sont à l'état sécurisé par défaut.

En savoir plus

Attribut	Description
Nom de la configuration technique	• glide.outbound_http_log.remplacer • glide.outbound_http_log.override.level
Applicabilité du module d'extension	Aucun
Risque de sécurité	Les en-têtes de demandes HTTP sortantes enregistrés avec des paramètres détaillés peuvent inclure des informations sensibles telles que des en-têtes d'autorisation ou des cookies. Ces informations peuvent être utilisées comme des informations d'identification pour accéder à la ressource demandée. Les utilisateurs ayant accès à la table Journaux HTTP sortants [sys_outbound_http_log] peuvent afficher ces informations. La gravité dépend du type de demandes sortantes effectuées.
Score du système de notation des vulnérabilités courantes (CVSS)	5

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	La propriété système **glide.outbound_http_log.override** vous permet de remplacer le niveau de journalisation des demandes HTTP sortantes. Une valeur **définie sur faux** définit le niveau de journal par défaut sur basique. Si **glide.outbound_http_log.override** est défini sur **true**, le niveau de journalisation est déterminé par la valeur de la propriété **glide.outbound_http_log.override.level** . Cette valeur peut être **basique**, **élevée** ou **toute**. Toutes les 3 sont des valeurs basées sur une chaîne/texte. Toute valeur autre que celles-ci est interprétée comme **basique**. Pour plus d'informations, reportez-vous à la section Configure outbound logging .
Dépendances et prérequis	Aucun
Type de données	• Booléen • Chaîne
Valeur de système de base	• Faux • <vide>
Valeur de secours	• Faux • <vide>
Valeur recommandée	• Faux • Élémentaire

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver les messages d'erreur SQL détaillé pour le processeur d'importation [Mis à jour dans Centre de sécurité 1.3]

Configurez cette propriété pour contrôler l'affichage des messages d'erreur SQL détaillés.

Si la propriété est définie sur **false**, un message d'erreur SQL détaillé s'affiche, ce qui peut révéler des informations sensibles. Pour éviter cela, définissez la propriété sur **vrai** pour afficher un message générique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.import.error_message.generic`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : définir la propriété sur **faux** active les messages SQL verbeux, ce qui peut entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

Fichiers et ressources

La catégorie des fichiers et des ressources garantit que les applications traitent les données de fichier non approuvées en toute sécurité et stockent les données non approuvées provenant de sources non approuvées avec des autorisations limitées dans un emplacement approprié.

Cela inclut des contrôles tels que la prévention du déni de service par le biais de types de fichiers volumineux ou inattendus, la validation du type de fichier et la prévention de la traversée du chemin.

Désactiver le téléchargement des fichiers infectés [Mis à jour dans Security Center 1.5 et 2.0]

Contrôlez si les utilisateurs peuvent télécharger des pièces jointes non analysées si le service antivirus est en panne ou inaccessible.

Lorsque la propriété est définie sur vrai, les `com.glide.snap.infected_download_allowed` utilisateurs peuvent toujours télécharger des pièces jointes non analysées au cas où le service antivirus serait en panne ou inaccessible. Cette situation expose potentiellement les utilisateurs au risque de télécharger un fichier malveillant, risquant ainsi d'infecter leur bureau, surtout s'il n'y a pas d'autre protection de point de terminaison installée sur l'appareil.

Assurez-vous que la propriété `com.glide.snap.infected_download_allowed` est définie sur false.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.snap.infected_download_allowed`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée faux peut exposer votre instance au téléchargement de fichiers malveillants.
Dépendances et prérequis	Aucun

Activer la notation et le filtrage d'e-mail indésirable [Mis à jour dans Centre de sécurité 1.3]

Installez le module d'extension Filtre d'e-mail (*com.glide.email_filter*) pour installer le filtrage des e-mails dans l'instance. Ce filtrage identifie les en-têtes existants, ce qui vous permet de décider quoi faire de l'e-mail en fonction de l'en-tête associé. Vous pouvez également définir la valeur *com.glide.email_filter* sur faux.

Chaque message envoyé via ServiceNow AI Platform les serveurs de messagerie est évalué pour déterminer s'il s'agit d'un spam.

Remarque :
Si une instance utilise un serveur de messagerie privé, cette rubrique ne s'applique pas. Pour plus d'informations, consultez Notation et filtrage d'e-mails indésirables.

Prérequis

Avant de définir cette propriété :

Définissez la propriété *glide.email.read.active* sur true. Pour plus d'informations, consultez Activer l'utilisation de votre propre serveur POP3 .

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.email_filter, glide.email.read.active
Type de configuration	Définition du système > Modules d'extension
Catégorie	Fichiers et ressources
Objectif	Pour appliquer le filtrage afin d'éviter le spamming d'e-mails.
Valeur recommandée	Ou:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• La propriété **glide.email.read.active** est définie sur **faux** • La propriété **glide.email.read.active** sur **true** et activez le module d'extension **Filtre d'e-mail** (com.glide.email_filter). Actif
Valeur par défaut	Aucun. Il s'agit d'un module d'extension, pas d'une propriété Glide, il n'y a donc pas de valeur par défaut.
Cote de risque de sécurité	8.1
Impact fonctionnel	Les e-mails ne sont jamais filtrés, bloqués ou mis en quarantaine de l'instance dans le cadre du score de courrier indésirable. Il est seulement noté puis envoyé à l'instance. Tout le filtrage est effectué dans l'instance avec le module d'extension Filtres d'e-mail.
Risque de sécurité	(Modéré) Les filtres d'e-mail permettent aux administrateurs d'utiliser un générateur de conditions ou un script conditionnel pour spécifier quand ignorer les e-mails entrants malveillants provenant d'un expéditeur connu/inconnu.
Références	Filtres d'e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

Activer l'analyse antivirus

La `com.glide.snap.enable_scan` propriété active la fonctionnalité d'analyse antivirus.

Définissez `com.glide.snap.enable_scan` la valeur recommandée sur **vrai** pour activer l'analyse antivirus.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.snap.enable_scan`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Fichiers et ressources
Objectif	Pour activer ou désactiver l'analyse antivirus sur une instance spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	vrai
Valeur par défaut	vrai
Type de données	Booléen
Risque de sécurité	(Élevé) L'analyse antivirus permet de protéger votre instance contre les infections de virus qui peuvent être introduites par des pièces jointes dans vos enregistrements système, telles que les incidents, les problèmes et les stories.
Cote de risque de sécurité	7.7

Restreindre les types de fichiers téléchargeables dans le contenu statique [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour activer les `glide.ui.strict_customer_uploaded_static_content` restrictions sur les types de fichiers qui peuvent être téléchargés lorsqu'ils ont été chargés à l'aide de la fonctionnalité Charger un fichier.

Vous utilisez cette propriété avec la `glide.ui.strict_customer_uploaded_content_types` propriété, ce qui crée une liste délimitée par des virgules des types de fichiers téléchargeables restreints.

⚠ Avertissement :
La valeur de cette propriété est un remplacement sans base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.strict_customer_uploaded_static_content`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Fichiers et ressources
Objectif	Pour s'assurer que les types de fichiers sécurisés peuvent être téléchargés à partir de l'application.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	3.1
Impact fonctionnel	Cette correction applique la restriction des téléchargements de fichiers en fonction des valeurs spécifiées dans la `glide.ui.strict_customer_uploaded_content_types` propriété.
Risque de sécurité	(Faible) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée utilisateur non approuvées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limiter la taille des pièces jointes dans les flux de formation et de prédiction pour les points de terminaison GraphQL [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La `glide.platform_ml_di.max_attachment_size_graphql` propriété contrôle la limite de taille maximale autorisée pour le renvoi de pièces jointes dans les points de terminaison GraphQL des flux de formation ou de prédiction.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.platform_ml_di.max_attachment_size_graphql`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	5,242,880
Valeur par défaut	5,242,880
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée de 5 242 880 ou moins, le renvoi de fichiers volumineux peut entraîner un déni de service (DoS).
Dépendances et prérequis	Aucun

Limiter la taille des pièces jointes dans les flux de formation et de prédiction [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La `glide.platform_ml_di.max_attachment_size` propriété contrôle la limite de taille maximale autorisée pour le renvoi de pièces jointes dans les flux de formation et de prédiction.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.platform_ml_di.max_attachment_size`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	4,000,000
Valeur par défaut	4,000,000
Catégorie	Fichiers et ressources

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si *glide.platform_ml_di.max_attachment_size* la valeur n'est pas définie sur la valeur recommandée de 4 000 000 ou moins, le renvoi de fichiers volumineux peut entraîner une attaque par déni de service (DoS).
Dépendances et prérequis	Aucun

Limiter la taille du corps de la réponse HTTP [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Configurez les *glide.http.response.get_body.limit.enabled* propriétés et *glide.http.response.get_body.limit* pour protéger votre instance contre *OutOfMemoryExceptions*.

Empêchez les exceptions OutOfMemoryExceptions qui peuvent résulter d'un corps de réponse de demande trop volumineux à l'aide des propriétés système **glide.http.response.get_body.limit.enabled** et **glide.http.response.get_body.limit** . Ces exceptions peuvent provoquer des attaques par déni de service (DOS) ainsi que d'autres problèmes susceptibles d'aider les attaquants à compromettre une instance. Si vous ne définissez pas ces propriétés sur les valeurs recommandées, votre instance peut être vulnérable aux exceptions OutOfMemoryExceptions et aux attaques par déni de service.

Pour protéger votre instance contre ces vulnérabilités de sécurité :

- Définissez la propriété système **glide.http.response.get_body.limit.enabled** sur **true**.
- Assurez-vous que la propriété système **glide.http.response.get_body.limit** est définie sur 524 288 000 mégaoctets (500 Mo).

En savoir plus

Attribut	Description
Nom de la configuration	• **glide.http.response.get_body.limit.enabled** • **glide.http.response.get_body.limite**
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Fichiers et ressources

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,1 • Détails du risque de sécurité : le fait de ne pas définir ces propriétés sur les valeurs recommandées pourrait rendre votre instance vulnérable aux `exceptions OutOfMemoryExceptions` et aux attaques par déni de service.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété réduit les risques d'une `exception OutOfMemoryException` due au chargement accidentel par un client d'un fichier volumineux dans la mémoire.

Limiter le nombre maximum de pièces jointes dans un e-mail

Configurez le nombre de pièces jointes d'e-mail entrant sur votre instance.

Cette`glide.email.inbound.max_attachment_count` propriété contrôle le nombre maximal de pièces jointes entrantes sur votre instance. Si cette propriété n'est pas définie sur la valeur recommandée de **30** ou moins, les e-mails entrants peuvent entraîner une dégradation des performances de l'instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.email.inbound.max_attachment_count`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	30
Valeur par défaut	30
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails du risque de sécurité : définir la valeur de la propriété sur plus de 30 peut entraîner des problèmes de dégradation.
Dépendances et prérequis	Aucun
Références	Email properties

Taille maximale autorisée de la pièce jointe [Mis à jour dans Centre de sécurité 1.3]

Configurez la `com.glide.attachment.max_size` propriété pour contrôler la taille maximale (en mégaoctets) autorisée pour une pièce jointe chargée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette propriété contrôle la taille maximale (en mégaoctets) d'une pièce jointe chargée. Si cette propriété n'est pas définie sur la valeur recommandée de **1024** (1 gigaoctet) ou moins, la plateforme peut accepter des fichiers volumineux qui pourraient remplir le stockage et entraîner une attaque par déni de service (DoS).

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.attachment.max_size`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1024
Valeur par défaut	1024
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété n'est pas définie sur **1 024** (1 gigaoctet) ou moins, la plateforme peut accepter des fichiers volumineux pouvant entraîner une attaque par déni de service.
Dépendances et prérequis	Aucun
Références	Attachment limit properties

Définir les types MIME enfant autorisés [nouveau dans Centre de sécurité 2.0]

Découvrez comment configurer la propriété sur un paramètre sécurisé afin que les `glide.security.mime.type.allowed_child_types` types de fichiers ne passent pas la vérification de type MIME (Multipurpose Internet Mail Extensions). Cela réduit le risque d'exécution de code à distance sur un fichier téléchargé.

La `glide.security.mime.type.allowed_child_types` propriété définit les types de fichiers MIME dont l'extension de fichier peut ne pas correspondre aux données d'un fichier chargé. Cela permet à ces types de fichiers de contourner la vérification du type MIME. La propriété accepte une liste de paires de types de fichiers séparées par des virgules, par exemple `application/zip=application/java-archive`. Dans cet exemple, si la propriété est définie sur une telle valeur, les fichiers avec une extension .zip qui sont techniquement .jar fichiers sont autorisés à passer la vérification de type MIME malgré l'incohérence. S'il n'est pas configuré correctement, ce contournement peut entraîner l'exécution de code à distance d'un fichier téléchargé. Par conséquent, il doit toujours être défini sur une chaîne vide (« ») sauf si un cas d'utilisation valide se présente. Par exemple, si un certain type MIME doit être autorisé sous une extension de fichier différente et est valide selon la configuration Tika, ces paires clé-valeur seront mises à jour dans le cadre de cette valeur de propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.mime.type.allowed_child_types`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	""
Valeur par défaut	""
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 4,6 • Score CVSS : moyen • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur la valeur sécurisée, des fichiers avec des configurations incorrectes peuvent entraîner l'exécution de code à distance d'un fichier chargé.
Dépendances et prérequis	Oui, lorsque `glide.security.mime.type.detection.allow_child_types` la valeur est définie sur vrai, les valeurs de cette propriété seront utilisées pour la validation par rapport à la liste configurée des types MIME enfant autorisés.
Impact fonctionnel	Pour prendre en charge les types MIME dont les extensions de fichier ne correspondent pas au contenu des fichiers mais sont valides selon les configurations de sous-type Tika dans `tika-mimetypes.xml`.

Valider le type MIME de fichier dans AttachmentCreator SOAP Web Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La `glide.attachment.enforce_security_validation` propriété détermine si les fichiers MIME (Multipurpose Internet Mail Extensions) sont soumis à validation.

Assurez-vous que les types MIME sont validés pour les pièces jointes afin d'empêcher le chargement de fichiers dangereux sur votre instance en utilisant des extensions de fichier incorrectes.

Définissez la propriété système **glide.attachment.enforce_security_validation** sur **true**. Lorsque la valeur est définie sur **vrai**, les fichiers sont chargés avec l'extension de type de fichier correcte.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.attachment.enforce_security_validation`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Fichiers et ressources
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : si la propriété est définie sur faux, il n'y a aucune validation pour les fichiers MIME pendant les chargements. Cela pourrait permettre aux fichiers malveillants d'être déguisés en changeant leur extension de fichier.
Dépendances et prérequis	Aucun
Références	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Impact fonctionnel	Définissez ce paramètre de sécurisation renforcée sur vrai pour exécuter les validations de type MIME et d'extension de fichier sur les pièces jointes chargées. Aucune validation n'est exécutée si cette propriété est définie sur faux. Cette propriété est définie sur vrai par défaut.

Code malveillant

La catégorie Code malveillant garantit que tous les efforts sont faits pour confirmer que votre code est exempt de vulnérabilités et de fonctionnalités indésirables.

Cela inclut la garantie d'une gestion sécurisée et appropriée des activités malveillantes, aucune attaque basée sur le temps, aucune communication sortante vers des destinations non approuvées et l'absence de code non autorisé ou contrôlé par des attaquants. Cette catégorie inclut les bibliothèques d'audit ou tierces de la base de code de l'application.

Bloquer les appareils mobiles racines ou jailbreakés

Sécurisez votre instance en empêchant tout accès non autorisé à partir d'appareils jailbreakés.

Utilisez cette propriété pour protéger votre instance contre tout `glide.sg.allow_rooted_jailbroken_device` accès non autorisé par des appareils jailbreakés. Si un utilisateur tente de s'authentifier dans une instance à l'aide d'une application mobile alors que cette propriété est définie sur **faux**, il reçoit l'alerte suivante : Cet appareil semble être jailbreaké et ne peut pas être utilisé pour accéder à cette instance. Veuillez contacter votre administrateur ServiceNow. L'application est gelée lorsque le message d'alerte est affiché, et la seule façon d'ignorer ce message est de sélectionner **Déconnecter**. Si cette propriété est définie sur **vrai,** les utilisateurs doivent s'authentifier dans une instance à l'aide d'un appareil jailbreaké.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sg.allow_rooted_jailbroken_device`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux
Catégorie	Code malveillant
Risque de sécurité	• Score de gravité : 4,5 • Score CVSS : moyen • Détails du risque de sécurité : Le manque de sécurité des appareils jailbreakés en fait une cible de choix pour les mauvais acteurs. Le fait que des entités non autorisées accèdent aux données de l'entreprise peut affaiblir la posture de sécurité d'un réseau d'entreprise.
Dépendances et prérequis	Aucun
Références	Contrôle d'accès

Activer la signature de code pour les données et les scripts de configuration d'application [Supprimé dans Centre de sécurité 1.3]

Gérez la signature de code pour les données et les scripts de configuration d'application sur votre instance.

La signature de code peut contribuer à améliorer la sécurité en validant les scripts et données de configuration sensibles des applications avant leur utilisation. La signature de code crée des signatures numériques pour les données, qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. Cette vérification empêche l'utilisation de scripts ou de données malveillants sur l'instance, ce qui pourrait entraîner une compromission totale de l'instance.

Utilisez la propriété pour gérer la signature de code pour les`com.snc.kmf.signature.validation.flag` données et les scripts de configuration d'application. Lorsque cette propriété doit être définie sur **vrai**, la signature de code est activée pour les données et les scripts de configuration d'application.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.kmf.signature.validation.flag`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Code malveillant
Risque de sécurité	• Score de gravité : 6 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **vrai** active la signature de code, ce qui contribue à améliorer la sécurité en validant les données et les scripts de configuration d'application sensibles.
Dépendances et prérequis	Aucun

Gestion des sessions

Cette catégorie examine la sécurité de l'état de l'application pour un utilisateur. Les sessions doivent être uniques à chaque individu, impossibles à deviner ou partager, et invalidées après des périodes d'inactivité ou lorsqu'elles ne sont pas nécessaires. Cela inclut des facteurs tels que les attributs de cookie pour les sessions basées sur les cookies, la génération de jetons de session, le stockage et les exigences de réauthentification fédérée.

Appliquer des politiques d'authentification continue aux sessions mobiles

Réduisez le risque de détournement de session en appliquant des politiques d'authentification continue aux sessions mobiles.

Assurez-vous que les utilisateurs mobiles utilisent la fonctionnalité de session d'assurance élevée du module d'extension Authentification Zero Trust - continue en définissant la propriété système **glide.zta.high_assurance.mobile.session.allowed** sur **faux**. Pour contourner les politiques d'authentification continue pour les sessions mobiles, définissez cette propriété sur **vrai**.

Définissez la propriété système **glide.zta.high_assurance.mobile.session.allowed** sur **faux**. Cette action réduit le risque de détournement de session et d'accès persistant si une session est compromise. Si cette propriété n'apparaît pas dans la table Propriétés système [sys_properties], la valeur par défaut est **faux**.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.zta.high_assurance.mobile.session.allowed
Applicabilité du module d'extension	Authentification Zero Trust - continue (com.snc.zero_trust_continuous_authentication)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	Si cette propriété système est définie sur **vrai**, la fonctionnalité de session d'assurance élevée n'est pas appliquée aux sessions mobiles. La réauthentification ne se produit pas comme défini dans les politiques pour les sessions à rôles élevés. Cela augmente le risque de détournement de session et d'accès persistant si une session est compromise.
Score du système de notation des vulnérabilités courantes (CVSS)	3.9
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Si elle est définie sur **vrai**, la fonctionnalité de session d'assurance élevée ne s'applique pas aux sessions mobiles, ce qui augmente le risque de détournement de session et d'accès persistant si une session est compromise.
Dépendances et prérequis	Aucun
Type de données	Booléen
Valeur de système de base	Faux
Valeur de secours	Faux
Valeur recommandée	Faux

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée du délai absolu d'expiration de la session [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour définir une durée de vie maximale pour les `glide.ui.user_cookie.max_life_span_in_days` cookies utilisateur créés lorsque les utilisateurs se connectent avec la case **Se souvenir de moi** cochée. Lorsque le cookie expire, les utilisateurs qui ont coché la case **Se souvenir de moi** sont obligés de s'authentifier à nouveau dans l'instance.

Il permet au cookie utilisateur d'être valide pour la durée de jours spécifiés, à compter de sa première émission. La valeur par défaut est de 30 jours et la limite maximale est de 365 jours.

Remarque :
Pour appliquer une durée de session maximale à toutes les sessions utilisateur actives, reportez-vous à la section Managing user sessions .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.user_cookie.max_life_span_in_days`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour forcer les utilisateurs qui ont coché la case **Se souvenir de moi** à se réauthentifier après des jours spécifiques.
Valeur recommandée	Inférieur ou égal à 30
Valeur par défaut	30 jours
Impact fonctionnel	Cette propriété impose une reconnexion obligatoire en évitant toute sorte de rotation des cookies après un délai donné.
Cote de risque de sécurité	4.2
Risque de sécurité	(Moyen) Le fait que les cookies utilisateur soient actifs pendant une durée indéterminée constituent un risque de sécurité et doivent expirer sur une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Définir les rôles d'exception de délai d'expiration de session active [nouveau dans Security Center 1.3]

Utilisez une propriété système pour exempter les rôles des limites de délai d'expiration de session active.

Utilisez la propriété système pour exempter les `glide.active.session.timeout.exception.roles` rôles d'une limite de délai d'expiration de session active. La fonction de délai d'expiration de la session active permet de s'assurer qu'une session détournée ne peut pas être utilisée indéfiniment sans fournir d'informations d'authentification. Il est recommandé de ne prendre en compte qu'une exception de limite de délai d'expiration de session active pour les rôles de compte d'intégration interne.

Configurez la propriété sur les `glide.active.session.timeout.exception.roles` rôles qui doivent être exemptés des délais d'expiration de session active. Cette valeur de propriété est une liste de rôles séparés par des virgules. La valeur par défaut est `edge_encryption,mid_server,maint`.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.active.session.timeout.exception.roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	edge_encryption,mid_server,maint
Valeur par défaut	edge_encryption,mid_server,maint
Valeur de secours	edge_encryption,mid_server,maint
Catégorie	Gestion des sessions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Envisagez une exception de limite de délai d'expiration de session active uniquement pour les rôles de compte d'intégration interne. Si un utilisateur est victime d'une tentative de détournement de session et qu'il dispose d'un rôle avec une exception, les attaquants utilisant cette session peuvent continuer à s'authentifier sur cette session indéfiniment. Cela peut augmenter l'impact d'un incident de sécurité en donnant à un attaquant plus de temps pour utiliser un compte piraté.
Dépendances et prérequis	Aucun

Activer UserCookie version 3.1 [Mis à jour dans Centre de sécurité 2.0]

Gérez la version de UserCookie activée sur votre instance pour sécuriser le stockage de la clé secrète dans le code source.

UserCookie v3 est généré uniquement lorsque la propriété *`glide.ui.secure.cookies.use_kmf is disabled`*. UserCookie v3 n'est pas sécurisé en raison du stockage de clé secrète pour HMAC dans le code source et identique pour tous les clients. Cela peut permettre à des acteurs malveillants d'utiliser cette clé secrète unique pour tenter de détourner des sessions utilisateurs. En définissant la propriété *`glide.ui.secure.cookies.use_kmf`* sur vrai, UserCookie v3.1 sera utilisé et la clé secrète sera stockée dans un stockage de sécurité tel que KMF.

En savoir plus

Attribut	Description
Nom de la configuration	*`glide.ui.secure.cookies.use_kmf`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : définir ceci sur **faux** est une vulnérabilité de sécurité car la clé secrète des codes d'authentification de message basés sur le hachage (HMAC) est stockée dans le code source.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer la réinitialisation du mot de passe aux demandes d'API [Mis à jour dans Centre de sécurité 1.5]

Gérez le fonctionnement de la fonctionnalité de réinitialisation du mot de passe sur votre instance.

Lorsqu'un utilisateur est marqué comme **devant être réinitialisé**, il doit fournir un nouveau mot de passe lors de la prochaine tentative d'authentification. Cette propriété contrôle si la réinitialisation du mot de passe est obligatoire avant d'effectuer des appels d'API. Si cette propriété **n'est** pas définie sur la valeur conseillée vrai, les comptes d'utilisateurs marqués comme **mot de passe à réinitialiser** peuvent toujours effectuer des opérations en interrogeant l'API de table via l'authentification de base. Cette faille de sécurité pourrait permettre une fuite d'informations si un compte inactif était compromis.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.api.user.reset_password.mandatory`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **faux** peut entraîner une fuite d'informations si un compte inactif est compromis.
Dépendances et prérequis	Aucun

Activer le marqueur de cookie HTTP uniquement [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour activer l'attribut `glide.cookies.http_only` HTTPOnly pour les cookies sensibles.

Utilisez l'attribut HTTPOnly pour empêcher les attaques, telles que le script de site à site, car il n'autorise pas l'accès au cookie à l'aide d'un script côté client, tel que JavaScript. Il n'élimine pas les risques de script de site à site, mais élimine certains vecteurs d'exploitation.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.cookies.http_only`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour atténuer le risque d'accès des scripts côté client au cookie protégé.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8
Impact fonctionnel	Cette correction ajoute un marqueur HTTPOnly supplémentaire sur les cookies de session, les protégeant ainsi contre le vol. • Si vous avez une fonctionnalité personnalisée qui nécessite JavaScript pour accéder au cookie de l'utilisateur, cela casse cette fonctionnalité. Cela ne devrait pas être le cas dans des circonstances normales. • Le ServiceNow AI Platform gère la gestion de session et il ne devrait pas y avoir de raison pour qu'un script personnalisé accède aux cookies de l'utilisateur.
Risque de sécurité	(Modéré) Les cookies de session dans l'application authentifient un utilisateur final et fournissent des autorisations d'accès implicites sur l'application. Cela signifie qu'il est nécessaire de les protéger contre le vol ou l'exportation. Les marqueurs HTTP Only protègent les cookies de session contre les injections JavaScript ou les vulnérabilités de script de site à site qui les volent.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Invalider la session après l'expiration du jeton OAuth [nouveau dans Security Center 2.0]

Configurez la propriété sur la valeur sécurisée pour empêcher les `glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled` utilisateurs de continuer à utiliser une session via des cookies après l'expiration du jeton OAuth utilisé pour créer la session.

Lorsque la `glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled` propriété n'est pas définie sur la valeur sécurisée true, un utilisateur peut continuer à utiliser une session via des cookies après l'expiration du jeton OAuth utilisé pour créer la session. Cela augmente le risque de fuite de cookies et de détournement de la session par un utilisateur malveillant pour accéder à des ressources non autorisées. Assurez-vous que la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled glide estdéfinie sur true. Si l'enregistrement n'existe pas dans la table sys_properties, la valeur par défaut est faux.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.authenticate.oauth.post.token.expiration.cookie_aut*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Pour les instances zboot, la propriété est vrai. Pour les instances de mise à jour, la propriété est false par défaut.
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 5,4 • Score CVSS : moyen • Détails du risque de sécurité : lorsque cette propriété n'est pas définie sur la valeur sécurisée true, un utilisateur peut continuer à utiliser une session même après l'expiration du jeton OAuth utilisé pour créer la session, ce qui augmente la probabilité que la session soit détournée par un utilisateur malveillant.
Dépendances et prérequis	Aucun
Impact fonctionnel	Vrai : l'authentification par cookie n'est respectée que jusqu'à l'expiration du jeton d'accès OAuth ; Après l'expiration, l'authentification n'est pas respectée. Faux : l'authentification par cookie est respectée même après l'expiration du jeton d'accès OAuth.

Minimiser le nombre de sessions interactives simultanées [Mis à jour dans Security Center 1.3]

Utilisez cette propriété avec le module d'extension Limite de sessions simultanées pour contrôler le nombre de sessions actives qui peuvent être ouvertes par un utilisateur.

Utilisez la propriété **Glide Authenticate Max Concurrent Interactive Sessions** avec le module d'extension **Limite de sessions simultanées** (*com.glide.limit.concurrent.sessions*) pour contrôler le nombre de sessions actives ouvertes pour un utilisateur. La valeur recommandée est **1**, ce qui réduit le nombre de sessions ouvertes (un nombre plus élevé augmente la probabilité qu'une session puisse être détournée).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.max.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1
Valeur par défaut	1
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : définir la valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module d'extension **Concurrent Interactive Sessions** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Limite de sessions simultanées dans tous les nœuds [Mis à jour dans Centre de sécurité 1.3]

Utilisez la `glide.authenticate.limit.concurrent.sessions.across.all.nodes` propriété avec le module d'extension Limite de sessions simultanées pour gérer le nombre de sessions suivies sur tous les nœuds.

Lorsque le module d'extension Sessions simultanées limites est actif, le nombre de sessions ouvertes peut être limité par utilisateur. Assurez-vous que lorsque ce module d'extension est actif, la propriété (**Glide authentifier la limite de sessions simultanées dans tous les nœuds**) est définie sur **vrai** afin que le nombre de sessions ouvertes soit suivi sur tous les nœuds au lieu d'un seul nœud d'application. Si cette propriété est définie sur **false**, plusieurs sessions peuvent être ouvertes sur plusieurs nœuds, ce qui augmente les risques de détournement de session.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.limit.concurrent.sessions.across.all.n`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Gestion des sessions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : lors de l'utilisation du module d'extension **Limite de sessions simultanées** , définir cette propriété sur **faux** permet d'ouvrir plusieurs sessions sur plusieurs nœuds, ce qui augmente le risque de vulnérabilité de sécurité comme un détournement de session.
Dépendances et prérequis	Aucun
Références	Sessions simultanées limites

Module d'extension Limite de sessions simultanées

Configurez le module d'extension com.glide.limit.concurrent.sessions pour réduire les risques de détournement de session sur votre instance.

Ce module d'extension permet à un administrateur de limiter le nombre de sessions actives par utilisateur et/ou rôle. Il est recommandé d'activer et de configurer ce module d'extension pour réduire la possibilité de détournement de session. Si ce module d'extension est activé et configuré, il y aura une limite au nombre de sessions ouvertes qui peuvent être détournées.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.limit.concurrent.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	module d'extension
Valeur recommandée	com.glide.limit.concurrent.sessions activé et configuré
Valeur par défaut	com.glide.limit.concurrent.sessions activé et configuré
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : Si ce module d'extension n'est pas actif, il y aura un risque accru de détournement de session.
Dépendances et prérequis	Aucun

Limiter la durée de vie de la session active de l'invité [nouveau dans Security Center 1.3]

Utilisez la `glide.guest.active.session.life_span` propriété pour contrôler la durée des sessions HTTP d'un invité actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La *glide.guest.active.session.life_span* propriété applique une durée de vie maximale sur les sessions HTTP d'invités actives, indépendamment de leur inactivité de session ou de la durée pendant laquelle un utilisateur est inactif avant l'expiration et la fermeture de sa session. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. Une valeur plus élevée pourrait permettre à un attaquant de rester plus longtemps dans une session volée, augmentant ainsi la possibilité d'un incident de sécurité. Cette propriété est limitée aux utilisateurs invités qui disposent d'un accès avec peu de privilèges à une instance.

Pour remédier à cette vulnérabilité de sécurité, définissez *glide.guest.active.session.life_span* une valeur supérieure à 0 et inférieure ou égale à 720.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.guest.active.session.life_span*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1 à 720 (minutes)
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : Définir la durée de vie maximale sur une valeur élevée donne à un acteur malveillant plus de temps au sein d'une instance au cas où il volerait une session.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette configuration applique la durée de vie maximale sur les sessions HTTP d'invités actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. La durée de vie maximale doit être supérieure au délai d'inactivité *glide.guest.session_timeout* (30 minutes par défaut).

Limiter les sessions interactives simultanées [Mis à jour dans Centre de sécurité 1.3]

Gérez le nombre de sessions interactives sur votre instance.

Cette propriété est destinée à être utilisée avec le module d'extension Limite de sessions simultanées (*com.glide.limit.concurrent.sessions*). Lorsque le module d'extension est actif et que la propriété est définie sur false, un utilisateur peut avoir un nombre illimité de sessions interactives simultanées sur une instance. Un plus grand nombre de sessions ouvertes signifie qu'il y a une grande possibilité de détournement de session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.limit.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	Faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : lorsque le module d'extension est actif et que la propriété est définie sur **false**, un utilisateur peut avoir n'importe quel nombre de sessions interactives simultanées, ce qui augmente la possibilité de détournement de session.
Dépendances et prérequis	Aucun
Références	Limiter les sessions interactives simultanées [Mis à jour dans Centre de sécurité 1.3]

Limiter la durée de vie de la session active des intégrations [nouveau dans Security Center 1.3]

La `glide.integrations.active.session.life_span` propriété applique la durée de vie maximale sur les sessions HTTP d'invités actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.integrations.active.session.life_span`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	0 à 720
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : une durée de vie maximale plus longue pourrait permettre à un attaquant de persister plus longtemps dans une session volée, augmentant ainsi la portée d'un incident de sécurité. Cette propriété est limitée aux intégrations qui disposent d'un accès avec peu de privilèges à une instance. Définissez la propriété `glide.integrations.active.session.life_span` Glide sur une valeur de 0 et inférieure ou égale à 720.
Dépendances et prérequis	Aucun

Limiter l'intervalle de jeton d'actualisation mobile d'accès à la session basée sur une politique [Nouveau dans Security Center 1.5]

Utilisez la `glide.authenticate.session_access.mobile.refresh_token_interval` propriété pour gérer la durée qui doit s'écouler avant qu'un utilisateur d'appareil mobile ne soit forcé de s'authentifier à nouveau.

Un utilisateur sera invité à s'authentifier à nouveau uniquement si l'administrateur a configuré les attributs du fournisseur d'identité dans la politique de session (les attributs peuvent varier à chaque connexion) et que l'utilisateur s'authentifie à l'aide de l'authentification unique (SSO). La valeur par défaut représente le temps en secondes dont dispose un utilisateur avant d'être réauthentifié. Une valeur par défaut plus élevée donne à un acteur malveillant plus de temps pour accéder à la session en cas de détournement de session.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.mobile.refresh_token_in`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1800 (secondes)
Valeur par défaut	1800 (secondes)
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si la politique ZTA est activée sur l'instance, les utilisateurs qui utilisent SSO pendant la connexion mobile seront forcés de se déconnecter et de se reconnecter après que la valeur par défaut de 1 800 secondes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	(30 minutes) aura été éclipsée. Si une valeur plus élevée est utilisée, les utilisateurs seront obligés d'attendre ce temps écoulé.
Dépendances et prérequis	Zero Trust : accès à la session basé sur des politiques
Impact fonctionnel	Ce paramètre régit le délai en secondes après la connexion, pendant lequel les utilisateurs seront obligés de se déconnecter des équipements mobiles s'ils utilisent l'authentification unique pour s'authentifier et si l'administrateur a configuré les attributs Identifier le fournisseur dans la politique d'accès à la session.

Limiter la durée de vie de la session active de l'interface utilisateur [nouveau dans Security Center 1.3]

La *glide.ui.active.session.life_span* propriété applique la durée de vie maximale sur les sessions HTTP authentifiées actives, quel que soit le délai d'expiration inactif.

Réduisez la portée des incidents de sécurité potentiels en diminuant la durée de vie des sessions HTTP actives. La propriété système **glide.ui.active.session.life_span** applique une durée de vie maximale sur les sessions HTTP actives, quel que soit le délai d'expiration inactif. Des durées de vie maximales plus longues peuvent permettre à un attaquant d'utiliser une session volée plus longtemps, augmentant ainsi la portée d'un incident de sécurité. La valeur par défaut de **0** désactive le délai d'expiration des sessions actives

Définissez le **glide.ui.active.session.life_span** sur une valeur comprise entre 1 et 720. Cette valeur représente la durée en minutes pendant laquelle les sessions HTTP peuvent rester actives.

Remarque :
La **glide.ui.active.session.life_span** est limitée à l'expiration de session d'interface utilisateur.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.ui.active.session.life_span*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1-720
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : une durée de vie maximale plus longue pourrait permettre à un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	attaquant de rester plus longtemps dans une session volée, augmentant ainsi la possibilité d'un incident de sécurité.
Dépendances et prérequis	Aucun
Impact fonctionnel	Applique la durée de vie maximale sur les sessions HTTP authentifiées actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. La durée de vie maximale doit être supérieure au délai d'inactivité glide.ui.session_timeout (30 minutes par défaut).

Limiter la durée de la session pour les sessions d'assurance élevée

Réduire le risque de prise de contrôle de compte dans les sessions à haute assurance en limitant la durée de la session

Réduisez le risque de prise de contrôle de compte dans les sessions de haute assurance en limitant la durée de la session. Passé le délai spécifié, les utilisateurs finaux doivent s'authentifier à nouveau.

Utilisez la propriété système **glide.zta.high_assurance.session.timeout** pour définir une durée, en minutes, après laquelle les utilisateurs doivent s'authentifier à nouveau. La valeur de cette propriété doit être comprise entre 1 et 480 minutes. Envisagez de limiter cette valeur à 30 ou moins pour réduire le risque de prise de contrôle de compte.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.zta.high_assurance.session.timeout
Applicabilité du module d'extension	Authentification Zero Trust - continue (com.snc.zero_trust_continuous_authentication)
Risque de sécurité	Des durées de session plus courtes réduisent le risque de prise de contrôle de compte en obligeant les utilisateurs à s'authentifier à nouveau.
Score du système de notation des vulnérabilités courantes (CVSS)	3.3
Évaluation du système commun de notation des vulnérabilités (CVSS)	Faible
Impact fonctionnel	Les utilisateurs des sessions d'assurance élevée doivent s'authentifier à nouveau à l'intervalle défini par cette propriété.
Dépendances et prérequis	Aucun
Type de données	Entier
Valeur de système de base	30
Valeur de secours	30
Valeur recommandée	30 ou moins

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Invalider de manière proactive les sessions inactives [nouveau dans Security Center 1.3 et mis à jour dans les versions 1.5 et 2.0]

La `glide.active.session.timeout.invalidate.session` propriété contrôle si une session de délai d'expiration est invalidée de manière proactive devant le serveur Tomcat.

Si `glide.active.session.timeout.invalidate.session` la valeur n'est pas définie sur **vrai**, il peut y avoir un petit intervalle de temps pendant lequel une session expirée n'est pas invalidée (60 secondes ou plus selon la taille de la file d'attente). Si une session est détournée, un attaquant peut être en mesure d'utiliser une session pendant cette courte période. Pour remédier à ce risque de sécurité, définissez sur `glide.active.session.timeout.invalidate.session`**vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.active.session.timeout.invalidate.session`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	Faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,6 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée vrai peut entraîner la non-validation d'une session expirée. Cela augmente les chances qu'un mauvais acteur détourne une session.
Dépendances et prérequis	Aucun

Rotation des identificateurs de session HTTP

Utilisez la propriété pour activer la `glide.ui.rotate_sessions` rotation des identificateurs de session HTTP afin de réduire les vulnérabilités de sécurité.

Si l'ID de session d'un utilisateur non authentifié ne change pas après l'authentification, une application Web est vulnérable à une attaque de fixation de session . Un utilisateur malveillant peut démarrer une session non authentifiée et donner l'ID de session associé à la victime. Une fois que la victime s'authentifie, l'utilisateur malveillant partage cette session authentifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.rotate_sessions*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette correction a modifié le SessionID lorsque l'utilisateur navigue d'une page non authentifiée vers des pages authentifiées. • Si vous utilisez un proxy ou codez en dur le SessionID lorsqu'un utilisateur se connecte pour la première fois, ou à toute autre fin, il peut y avoir un impact potentiel sur les fonctionnalités. • Si vous utilisez le module d'extension SAML 2.0 pour l'authentification unique, il peut interférer avec le partage d'informations de session entre l'instance et le fournisseur d'identité. Dans ce cas, vous pouvez définir cette propriété sur faux.
Risque de sécurité	(Modéré) SessionID est utilisé pour traiter et authentifier l'utilisateur d'instance en conservant l'état de la session sur le navigateur. Ainsi, SessionID est considéré comme une donnée sensible et doit être sécurisé par défaut. La rotation de session est un contrôle de sécurité qui applique la modification de sessionID chaque fois que l'utilisateur navigue de pages non authentifiées vers des pages authentifiées.
Références	Authentification avec SAML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le nombre de sessions interactives simultanées [Mis à jour dans Security Center 1.3]

Utilisez cette propriété avec le module d'extension Limite de sessions simultanées pour contrôler le nombre de sessions actives qui peuvent être ouvertes par un utilisateur.

Utilisez la propriété **Glide Authenticate Max Concurrent Interactive Sessions** avec le module d'extension **Limite de sessions simultanées** (*com.glide.limit.concurrent.sessions*) pour contrôler le nombre de sessions actives ouvertes pour un utilisateur. La valeur recommandée est **1**, ce qui réduit le nombre de sessions ouvertes (un nombre plus élevé augmente la probabilité qu'une session puisse être détournée).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.max.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1
Valeur par défaut	1
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : définir la valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module d'extension **Concurrent Interactive Sessions** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Minimiser la durée du délai d'expiration d'activité de la session [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour désigner, en minutes, la valeur du délai d'expiration de l'activité `glide.ui.session_timeout` .

La définition de cette propriété a plusieurs impacts fonctionnels :

- Plus le délai d'expiration de la session spécifiée est long, plus la quantité de mémoire utilisée pendant une session de traitement est importante. Le système de base utilise une durée de délai d'expiration Apache Tomcat par défaut de 30 minutes.
- Ils ServiceNow AI Platform déconnectent toujours les utilisateurs avec Remember Me. Après 30 minutes d'inactivité dans l'application, la plateforme déconnecte automatiquement l'utilisateur, sauf si la case **Se souvenir de moi** dans la page de connexion est cochée. Ce qui est différent, c'est qu'ils ne se reconnectent pas pour continuer.
- Si des jauges ou du contenu sur les pages d'accueil des utilisateurs s'actualisent automatiquement, ce délai peut ne jamais être atteint.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.session_timeout`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour appliquer le délai d'expiration de session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	Délai d'expiration spécifié par l'utilisateur en minutes. 60 minutes est la valeur recommandée, mais cette valeur peut varier en fonction de la fonctionnalité et des exigences de sécurité. Ne définissez pas cette valeur sur plus d'un jour.
Cote de risque de sécurité	7.5
Impact fonctionnel	Cette correction applique l'expiration en temps opportun du compte utilisateur. Aucun impact sur les fonctionnalités, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Élevé) Le fait que les sessions utilisateur soient actives pendant une durée indéfinie constituent un risque pour la sécurité et doivent expirer sur une configuration basée sur le temps.
Références	Gérer les sessions utilisateur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée du délai d'expiration de la fenêtre de session [Mis à jour dans Centre de sécurité 1.3]

Utilisez la `glide.ui.user_cookie.life_span_in_days` propriété pour définir le délai d'expiration du cookie Se souvenir de moi. La valeur par défaut est de 15 jours et la limite maximale est de 30 jours.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.user_cookie.life_span_in_days`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour permettre l'expiration par défaut du cookie **Se souvenir de moi** .
Type de données	Entier
Valeur recommandée	15
Valeur par défaut	15
Cote de risque de sécurité	4.9
Impact fonctionnel	Cette propriété est activée par l'utilisateur final lorsque celui-ci coche la case **Mémoriser** mon nom sur la page de connexion et se connecte à .ServiceNow AI Platform
Risque de sécurité	(Modéré) Le fait que les cookies utilisateur soient actifs pendant une durée indéterminée constituent un risque de sécurité et doivent expirer sur une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Cryptographie stockée

Cette catégorie se concentre sur le chiffrement des données stockées. Elle englobe plusieurs aspects clés, tels que l'utilisation d'algorithmes et de modules cryptographiques établis, la garantie de la génération correcte de valeurs pseudo-aléatoires, la mise en œuvre d'un cryptage basé sur la classification des données et le stockage et l'isolement sécurisés du matériel clé.

Activer le chiffreur Glide KMF [supprimé dans le centre de sécurité 1.3.2]

Gérez les chiffreurs utilisés pour les champs Password2 sur votre instance.

Utilisez la propriété pour définir le`glide.kmf.encrypter.enabled` chiffreur KMF comme chiffreur par défaut pour les champs Password2. Cette propriété garantit que des normes de chiffrement fortes et conformes sont utilisées au lieu d'un chiffreur hérité. Pour vous assurer que le chiffreur KMF est utilisé au lieu du chiffreur hérité, définissez cette propriété sur **vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.kmf.encrypter.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Cryptographie stockée
Risque de sécurité	• Score de gravité : 4,9 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **vrai** garantit que le chiffreur KMF est utilisé au lieu du chiffreur hérité.
Dépendances et prérequis	Aucun
Références	Chiffrement Password2 avec Key Management Framework (KMF)

Désactiver l'utilisation de l'algorithme de chiffrement TripleDES/3DES

Évitez les risques de sécurité liés aux méthodes de chiffrement obsolètes en désactivant l'utilisation de l'algorithme de chiffrement TripleDES/3DES.

Désactivez l'utilisation de la norme 3DES ou Triple-DES (Triple Data Encryption Standard) héritée et déconseillée sur votre instance, ce qui peut entraîner la perte et la fuite d'informations sensibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le National Institute of Standards and Technology (NIST) a déconseillé l'utilisation de Triple DES (3DES) pour crypter les données. Pour plus de détails, reportez-vous à la norme NIST 800-131A Rév. 2. 3DES est désormais interdit pour le chiffrement dans les systèmes fédéraux. À l'avenir, TDES ne pourra être utilisé qu'à des fins historiques, telles que le déchiffrement d'anciens messages, le désencapsulage de clés et la vérification MAC.

La propriété système **glide.security.3des.encryption.allow** contrôle si le chiffrement 3DES est activé sur votre instance, mais plusieurs étapes peuvent être nécessaires pour vérifier que votre instance est prête pour la dépréciation. Consultez KB1704481 pour plus d'informations sur le processus de dépréciation avant de définir cette propriété.

En savoir plus

Attribut	Description
Nom de la configuration technique	glide.security.3des.encryption.allow
Applicabilité du module d'extension	Aucun
Risque de sécurité	L'utilisation d'un cryptage obsolète et faible comme 3DES peut entraîner la perte et la fuite d'informations sensibles.
Score du système de notation des vulnérabilités courantes (CVSS)	4.2
Évaluation du système commun de notation des vulnérabilités (CVSS)	Moyen
Impact fonctionnel	Définir cette propriété sur **faux** permet d'empêcher votre instance d'utiliser un chiffrement obsolète et faible. Cela affecte la façon dont les données Password2 sont stockées. Consultez KB1704481 pour plus d'informations sur l'impact fonctionnel de l'obsolescence de la 3DES.
Dépendances et prérequis	Effectuez les tâches décrites dans KB1704481 avant de modifier la valeur de cette propriété.
Type de données	Booléen
Valeur de système de base	faux
Valeur de secours	Faux
Valeur recommandée	Faux

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Empêcher l'utilisation des clés 3DES [nouveau dans Security Center 7.0]

Désactivez l'utilisation des clés statiques 3DES sur votre instance avec une propriété système.

Utilisez la `glide.security.3des.static_keys_usable` propriété système pour désactiver l'utilisation des clés statiques 3DES sur votre instance. Cette propriété doit être définie automatiquement par une tâche planifiée, dont l'état peut être vérifié via la propriété `glide.security.3des.removal_job_status`. Dans les cas où cette propriété n'est pas configurée sur **faux**, une fois que la tâche planifiée s'exécute et que l'état est KEYS_DEACTIVATED, la tâche planifiée attend que cette propriété soit configurée sur **faux** avant de poursuivre la suppression des clés statiques 3DES.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que le *glide.security.3des.static_keys_usable* existe dans la table Propriétés système [sys_properties] et qu'il est défini sur **la valeur faux**. Consultez KB1704481 pour plus d'informations sur l'obsolescence de 3DES.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.security.3des.static_keys_usable*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Valeur de secours	vrai
Catégorie	Cryptographie stockée
Risque de sécurité	• Score de gravité : 5 • Score CVSS : moyen • 3DES est déconseillé, et l'utilisation de clés statiques 3DES et 3DES en dehors de la rétrocompatibilité temporaire n'est pas recommandée. L'utilisation continue peut conduire à des situations de divulgation d'informations sensibles si un utilisateur devait obtenir l'accès à des données cryptées.
Impact fonctionnel	Lorsqu'il est défini sur **faux**, il peut y avoir des situations peu probables où le code et les données résidant sur l'instance encore utilisée par les clés statiques 3DES sont désormais inaccessibles.
Dépendances et prérequis	Aucun

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Validation, nettoyage et codage

La validation, le nettoyage et le codage abordent la validation d'entrée pour prévenir les vulnérabilités telles que le script de site à site (XSS), l'injection SQL et d'autres attaques.

Ce contrôle garantit que la validation d'entrée et le codage de sortie sont en place et correctement configurés, par exemple, le codage ou l'échappement des données de sortie. Cette catégorie comprend également des vérifications d'éléments tels que la désérialisation des objets et la validation positive via des listes d'autorisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisez les liens HTML vers des domaines de confiance dans les champs de description du module de l'espace de travail Impact [nouveau dans Security Center 7.0]

Utilisez une propriété système pour nettoyer le code HTML autorisé dans les champs de description. Cette propriété limite les liens autorisés uniquement à ceux provenant des domaines de confiance répertoriés dans la propriété.

Remarque :
Ce paramètre de durcissement ne fait pas partie de la base de référence de durcissement. Il n'apparaît pas dans les pages de sécurisation renforcée du Centre de sécurité et affecte votre score de sécurisation renforcée.

Le module Impact Workspace autorise le HTML dans un certain nombre de champs liés à la description. Lorsqu'elle est configurée, la *sn_impact_common.whitelisted.url_HTML_injection* propriété système contient une liste de noms de domaines séparés par des virgules. Les champs de description du module de l'espace de travail d'Impact peuvent contenir des HREF avec des URL uniquement des domaines répertoriés dans la propriété.

Assurez-vous que la *sn_impact_common.whitelisted.url_HTML_injection* propriété système est définie sur une liste de noms de domaines séparés par des virgules qui représentent les domaines autorisés dans les URL de référence HTTP des champs de description du module Espace de travail d'Impact.

Pour interdire les HREF dans ces champs, définissez la propriété sur une chaîne vide. Si la propriété n'existe pas dans la table Propriétés système [sys_properties], elle utilise par défaut cette liste : servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_impact_common.whitelisted.url_HTML_injection*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Liste de chaînes
Valeur recommandée	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com
Valeur par défaut	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com
Valeur de secours	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Si un domaine non approuvé est ajouté à la propriété, ces champs peuvent contenir des liens vers des sources risquées pouvant entraîner des attaques par injection HTML. Le risque exact dépend de l'instance client.
Impact fonctionnel	Si la propriété est vide, aucun HREF n'est autorisé dans le texte du champ et tous les HREF sont supprimés. Tous les liens utilisant des domaines non répertoriés dans la propriété sont supprimés. Une valeur incorrecte pour ce champ peut entraîner des données corrompues pour les champs affectés.
Dépendances et prérequis	Si la `sn_impact_common.blacklist_tags_HTML_injection` propriété système contient des balises HTML qui entourent les liens HREF, tous les liens à l'intérieur de ces balises seront supprimés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès à l'API de script GlideSystemUserSession [Mise à jour dans Centre de sécurité 1.3 et 2.0]

L'API scriptable GlideSystemUserSessionSandbox appelable par le client expose les méthodes GlideSystemUserSession addErrorMessageNoSanitization et addInfoMessageNoSanitization au bac à sable JavaScript. Cela permet à tous les utilisateurs d'appeler cette méthode via un script.

`gs.addErrorMessageNoSanitizationMessaging()` et `gs.addInfoMessageNoSanitization()` sont utilisés dans l'environnement de script pour la journalisation et les notifications. Ces deux éléments sont disponibles dans le bac à sable si cette propriété n'est pas définie sur la valeur recommandée faux Le bac à sable est un environnement de script avec peu de privilèges disponible pour les utilisateurs non authentifiés et sans rôle. Ces deux méthodes peuvent être utilisées pour afficher une entrée non expurgée à un utilisateur. L'affichage d'une entrée non expurgée à l'utilisateur est dangereux, car l'entrée non expurgée peut contenir du code dangereux qui s'exécute dans le navigateur de l'utilisateur. Cela peut être utilisé pour les attaques XSS réfléchies traditionnelles. Les attaques XSS réfléchies peuvent être utilisées dans plusieurs scénarios, y compris le détournement de session.

Définissez **glide.sandbox.usersession.allow_unsanitized_messages** propriété système sur **faux**. Si cette propriété n'est pas enregistrée dans la table Propriétés système [sys_properties], créez-en une.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sandbox.usersession.allow_unsanitized_messages`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Cette propriété empêche l'appel de messages d'information ou d'erreur non expurgés dans une session utilisateur bac à sable.
Type	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Cote de risque de sécurité	8.1
Impact fonctionnel	Définir la propriété avec la valeur false n'entraînera aucune création de message ou journalisation si ces fonctions sont appelées.
Risque de sécurité	(Élevé) Sans nettoyage approprié, du contenu potentiellement dangereux peut être accessible et la fonction d'erreur non nettoyée est disponible pour le script.
Références	Contrôle d'accès

Désactiver les balises JavaScript dans le HTML intégré [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour désactiver la prise en charge de l'incorporation `glide.ui.security.codetag.allow_script` du code JavaScript HTML créé à l'aide de la balise [code].

Il ServiceNow AI Platform atténue de nombreuses attaques par injection et cross-site en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire et soumettre des entrées au format HTML pour les champs journal. Toutefois, les champs journaux peuvent afficher le texte inclus dans les balises de code au format HTML. Assurez-vous que la propriété existe dans la table sys_properties et qu'elle `glide.ui.security.codetag.allow_script` est définie sur faux.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur **vrai**, les utilisateurs malveillants peuvent écrire du code JavaScript HTML nuisible qui peut être exécuté sur un navigateur client différent après le rendu des champs de journal.
- Définissez cette propriété sur **faux** afin que les administrateurs puissent empêcher les champs journaux de rendre du code JavaScript HTML en désactivant la prise en charge de la balise [code].

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.security.codetag.allow_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Protège contre le script de site à site et l'exécution de scripts malveillants
Valeur recommandée	Faux
Valeur par défaut	Faux
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette remédiation impose l'échappement de JavaScript dans l'interface utilisateur et rend les résultats encodés à l'utilisateur. Elle peut avoir un impact fonctionnel basé sur l'interaction de l'utilisateur de l'instance avec les données obtenues.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Restreindre la balise CODE dans les champs de journal Afficher les entrées du champ journal au format HTML Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le gestionnaire de sécurité Java renforcé [nouveau dans le centre de sécurité 1.3]

La `glide.security.manager` propriété contient le nom de classe Java du gestionnaire de sécurité Java actuel.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.manager`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	`com.glide.sys.security.ContextualSecurityManager`
Valeur par défaut	`com.glide.sys.security.ContextualSecurityManager`
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : si `glide.security.manager` cette option n'est pas définie sur la valeur conseillée , `com.glide.sys.security.ContextualSecurityManager`l'instanc utilise peut-être un gestionnaire de sécurité Java obsolète dont les politiques de sécurisation renforcée attendues sont manquantes. Sans ce durcissement, un acteur malveillant disposant d'un accès à l'exécution de script pourrait obtenir une exécution de code à distance sur l'instance.
Dépendances et prérequis	Aucun

Appliquer l'assainissement HTML [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour appliquer le `com.glide.security.check_unsanitized_html` comportement de nettoyage des champs translated_html à un niveau global pour les affectations de champs.

HTML est l'un des types qui peuvent être affectés aux champs de dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet de formater le contenu à l'aide de balises HTML (par exemple, `<p>`, `<a href>`, `<b><font><img>`, ,). Pour éviter les activités malveillantes, certaines balises HTML peuvent être interdites à l'aide d'une liste de blocage. Cette propriété empêche l'utilisation de balises interdites dans les champs translated_html de votre instance.

- Définissez cette propriété à **appliquer** pour appliquer le comportement de nettoyage de translated_html champs.
- Définissez la propriété sur **désactiver** pour désactiver l'assainissement HTML afin d'autoriser le blocage des balises HTML sur translated_html champs.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.security.check_unsanitized_html`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Empêche l'utilisation de balises HTML non sécurisées pour se protéger contre les attaques telles que le script de site à site.
Type	Chaîne
Valeur recommandée	appliquer
Valeur par défaut	appliquer
Cote de risque de sécurité	7.3
Impact fonctionnel	Cette correction applique l'assainissement HTML sur l'interface utilisateur et renvoie les champs HTML traduits à l'utilisateur. Cela peut avoir un impact sur la lisibilité et le formatage.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Assainisseur HTML

Garantir que la recherche contextuelle ne contient pas de redirection non validée [nouveau dans Security Center 7.0]

Empêchez les résultats de Recherche contextuelle de contenir des liens de référence en dehors du domaine actuel avec une propriété système.

Le module d'extension Recherche contextuelle affiche les résultats de la recherche dans une nouvelle fenêtre à l'aide de la page de l'interface utilisateur. Cette page d'interface utilisateur contient un lien de référence qui peut être défini en fournissant une valeur à `sysparm_url`. Lorsque la `com.snc.contextual_search.cxs_new_window.force_relative_link` propriété système est définie sur **vrai**, `sysparm_url` elle ne peut contenir que des liens relatifs au domaine actuel. Cette restriction empêche la page d'interface utilisateur d'être utilisée comme une redirection non validée vers un site Web contrôlé par des attaquants. Lorsque la propriété est définie sur **faux**, `sysparm_url` peut créer un lien vers n'importe quel site web.

Définissez la `com.snc.contextual_search.cxs_new_window.force_relative_link` propriété sur **vrai**. Si la propriété n'existe pas dans la table Propriétés système [sys_properties], la valeur par défaut est **faux**. Si la propriété existe dans la table, elle est définie par défaut sur **true**.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.contextual_search.cxs_new_window.force_relative_l`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur de secours	Faux
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : moyen • Lorsqu'il est défini sur **faux**, `sysparm_url` il peut être lié à n'importe quel site web, ce qui permet d'utiliser la page de l'interface utilisateur comme une redirection non validée vers un site web contrôlé par l'attaquant.
Impact fonctionnel	Quand elle est définie sur **vrai**, `sysparm_url` elle est autorisée à contenir uniquement des liens relatifs au domaine actuel. Cette restriction signifie que la page de l'interface utilisateur ne peut être liée qu'à des pages Web du domaine actuel. Toutefois, la page d'interface utilisateur est destinée à afficher les résultats de recherche du domaine actuel et ne doit être liée qu'au domaine actuel.
Dépendances et prérequis	Le module d'extension Recherche contextuelle (com.snc.contextual_search) doit être actif.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver AJAXEvaluate

Utilisez pour `glide.script.allow.ajaxevaluate` protéger l'API système contre les vulnérabilités de l'exécution du script client via les appels AJAX.

L'élévation au rôle security_admin est requise pour modifier la propriété.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script.allow.ajaxevaluate`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour empêcher un utilisateur d'exécuter des scripts en tant que privilège d'administrateur.
Valeur recommandée	Faux
Valeur par défaut	Faux
Type de configuration	Booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	Ce rattrapage force la désactivation du processeur AJAXEvaluate. Cela peut avoir un impact sur les fonctionnalités si vous utilisez explicitement le processeur d'évaluation AJAX dans le cadre de scripts personnalisés.
Risque de sécurité	(Élevé) Le processeur AjaxEvaluator exécute les scripts clients dans le bac à sable, mais il existe plusieurs propriétés supplémentaires qui peuvent permettre d'étendre le champ d'application des activités dans le bac à sable.
Cote de risque de sécurité	7.3
Références	Cette propriété appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution de scripts provenant du client, telles que `glide.script.allow.ajaxevaluate`. Pour plus d'informations, consultez Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5]

Si les personnalisations ne nécessitent pas l'expansion de l'entité, utilisez la propriété pour désactiver complètement l'expansion de l'entité `glide.stax.allow_entity_resolution` externe. Le code XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

Désactivez l'expansion de l'entité sur votre instance pour la sécuriser contre les attaques telles que la capacité à lire des fichiers système et le déni de service. Utilisez la propriété système pour interdire le développement des entités XML lors de l'analyse par l'analyseur de diffusion (XMLDocument2).

Définissez la propriété système **glide.stax.allow_entity_resolution** sur **faux** pour désactiver l'expansion de l'entité sur votre instance. Si cette propriété n'apparaît pas dans la table Propriétés système [sys_properties], la valeur par défaut est **vrai**. Créez l'enregistrement de propriété et définissez la valeur sur **faux** pour modifier sa valeur.

Prérequis

Avant de définir cette propriété :

- Définissez les propriétés et `glide.xml.entity.whitelist.enabledglide.stax.whitelist_enabled` sur vrai. Pour en savoir plus, reportez-vous aux sections Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0] et Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mis à jour dans Centre de sécurité 1.3].
- Définissez une liste de FQDN délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL pouvant être atteintes à l'aide du traitement d'entité XML. Pour en savoir plus, consultez Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.stax.allow_entity_resolution`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour se défendre contre une attaque XML Entity Expansion/Billion Laugh.
Valeur recommandée	Faux
Valeur par défaut	vrai
Impact fonctionnel	Si la personnalisation utilise l'expansion de l'entité, elle ServiceNow AI Platform peut bloquer tout traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources système.
Solution de contournement	Si la personnalisation nécessite le développement de l'entité, définissez cette propriété sur true et suivez les étapes décrites à la rubrique Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mis à jour dans Centre de sécurité 1.3].

Pour en savoir plus sur l'ajout ou la création d'une propriété système, voir Add a system property

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Désactiver l'URL du contenu externe [Mis à jour dans Centre de sécurité 2.0]

Gérez la façon dont les métadonnées de liens externes sont utilisées dans votre instance avec la Messagerie instantanée de Connexion.

Utilisez la propriété pour gérer les `glide.ui.url.external.content` métadonnées des liens externes dans votre instance. Si la propriété est définie sur la valeur recommandée **faux**, aucune métadonnée de lien externe n'est affichée. Si la valeur est définie sur **vrai** , Connect Chat les métadonnées des liens externes sont récupérées à partir de sources telles que YouTube ou des articles d'actualité pour rendre des messages plus riches. Cela peut entraîner des attaques de falsification de requête côté serveur (SSRF).

Assurez-vous que la propriété `glide.ui.url.external.content` Glide existe et qu'elle est définie sur la valeur faux. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.url.external.content`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	vrai
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **vrai** pourrait exposer votre instance à des attaques de falsification de requête côté serveur (SSRF).
Dépendances et prérequis	Aucun
Références	Connect Chat

Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]

La `glide.ui.attachment.download_mime_types` propriété forcera le téléchargement de la liste spécifiée de types de fichiers dangereux sur le client et leur non-affichage aligné dans le navigateur.

Si la propriété `glide.ui.attachment.force_download_all_mime_types` est définie sur true, la `glide.ui.attachment.download_mime_types` propriété est alors remplacée afin que tous les types MIME soient téléchargés plutôt qu'affichés par le navigateur. Par exemple, le téléchargement de texte/html force un fichier HTML à être téléchargé sur le client en tant que fichier plutôt que d'être affiché en ligne dans le navigateur, empêchant ainsi une attaque XSS. XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué.

Nouvelle correction : assurez-vous que la propriété `glide.ui.attachment.force_download_all_mime_types` est définie sur true. Si la propriété n'existe pas dans la table sys_properties, la valeur par défaut est faux.

Remarque :
Le rôle security_admin est requis pour modifier la propriété.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.attachment.download_mime_types`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	La gestion correcte de la liste des types de fichiers dangereux qui ne peuvent pas être affichés dans le navigateur empêchera les attaques de script de site à site (XSS).
Valeur recommandée	Liste des types MIME applicables ou valeur recommandée : text/html,image/svg,image/svg+xml,application/xml
Valeur par défaut	Liste des types MIME applicables pour la valeur par défaut : text/html,image/svg,image/svg+xml,application/xml
Type de configuration	Chaîne : toutes les valeurs séparées par des virgules des types MIME d'application.
Impact fonctionnel	Cette correction renforce la performance des contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une ServiceNow AI Platform application. Il n'y a pas d'impact potentiel, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Modéré) Les attaquants peuvent abuser des types MIME et placer du contenu de script non souhaité dans la pièce jointe du côté de la victime pour capturer des informations sensibles. La possibilité d'avoir des XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés, tels que l'administrateur, où un mouvement plus latéral peut être effectué. Dans le contexte actuel, renseignez la propriété avec une liste de types MIME séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur.
Cote de risque de sécurité	6.4
Propriétés connexes	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
Références	Définir les types MIME téléchargeables restreints [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0].

Désactiver le code HTML intégré [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour désactiver la prise en charge de l'incorporation *glide.ui.security.allow_codetag* du code HTML créé à l'aide de la balise [code].

Désactiver la prise en charge de l'affichage du code HTML incorporé à l'aide de la balise [code]. Cette balise permet au HTML rendu de s'afficher dans les champs de journal et peut entraîner des attaques de script de site à site (XSS). Ces attaques peuvent permettre à des scripts étrangers de s'exécuter sur une session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent utiliser ces scripts pour voler des informations de session et des données sensibles. Le langage HTML n'a pas été conçu pour séparer le script du formatage, donc permettre le HTML contrôlé par l'utilisateur dans n'importe quel système comporte un risque inhérent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir la **glide.ui.security.codetag.allow_script** sur **faux** est conforme et réduit considérablement ce risque, mais un petit risque demeure. Il désactive uniquement la partie script d'une balise de `code` et s'appuie sur le nettoyage de toutes les conventions connues du script dans le HTML.

Définissez la propriété système **glide.ui.security.allow_codetag** sur **false** pour interdire complètement aux champs et formulaires journaux d'afficher du contenu HTML rendu.

Il ServiceNow AI Platform atténue de nombreuses attaques par injection et cross-site en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire/soumettre d'entrées au format HTML pour les champs journal. Mais les champs journaux peuvent rendre le texte entouré de balises de code en HTML.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur `vrai`, les utilisateurs malveillants peuvent écrire du code JS HTML nuisible qui peut être exécuté sur un navigateur client différent après le rendu des champs de journal.
- Définissez cette propriété sur `faux` afin que les administrateurs puissent empêcher les champs de journal de rendre le code HTML en désactivant la prise en charge de la balise `[code]`.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.security.allow_codetag
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre le script de site à site et l'exécution de scripts malveillants
Valeur recommandée	Faux
Valeur par défaut	vrai
Cote de risque de sécurité	4.2
Impact fonctionnel	Cette correction force l'encodage HTML à se produire sur l'interface utilisateur et rend les résultats encodés à l'utilisateur. Cette propriété est définie sur `vrai` par défaut. Dans cet état, votre instance affiche le rendu HTML dans les champs de journal et les formulaires. Si cette propriété est définie sur `false`, HTML n'est pas affiché correctement et les balises HTML peuvent apparaître dans les champs de journal des formulaires. Elle peut avoir un impact négatif sur les fonctionnalités et sur les interactions des utilisateurs avec les données résultantes.
Risque de sécurité	(Moyen) La validation de l'entrée doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	de s’exécuter sur une session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l’utiliser pour voler des informations de session et des données sensibles.

Activer l’assainisseur HTML dans Agent virtuel [Mise à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour activer HTMLSanitizerService `com.glide.cs.html.sanitizer.enabled` .

Cette propriété contrôle si HtmlSanitizerService est activé. Si `com.glide.cs.html.sanitizer.enabled` la valeur n’est pas définie sur vrai, une attaque de script de site à site stocké (XSS) est possible dans le client Web VA.

En savoir plus

Avertissement :
Il s’agit d’une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu’elle a été modifiée. Il n’est pas réversible.

Attribut	Description
Nom de la propriété	`com.glide.cs.html.sanitizer.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêche l’application contre les attaques de script de site à site et d’injection HTML.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8
Impact fonctionnel	Cette correction applique un mécanisme de codage de sortie HTML avant que les données utilisateur ne soient restituées à l’utilisateur. Si le client dispose d’une personnalisation qui implique le rendu de l’attribut HTML ou des données de contenu, il y a un impact sur la fonctionnalité.
Risque de sécurité	(Élevé) L’entrée de l’utilisateur doit être traitée en toute sécurité lorsque les données sont stockées et traitées sur l’application. Cela réduit les attaques de script de site à site côté client en encodant les données de sortie.

Pour en savoir plus sur l’ajout ou la création d’une propriété système, reportez-vous à la section Add a system property .

Activer la protection contre l'interpolation de Jelly JS

Utilisez la `glide.ui.jelly.js_interpolation.protect` propriété pour vous assurer que tout JavaScript sur le point d’être exécuté sur une page Jelly est protégé de l’injection à l’aide de l’interpolation Jelly.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous définissez la propriété sur **true**, une application passe par une arborescence de scripts Jelly (imbriquée). Il enveloppe les expressions Jelly potentiellement dangereuses avec un filtre qui :

- Échappe à leurs résultats pour être en sécurité, ou
- Si leur sécurité ne peut pas être garantie, génère une SecurityException, car l'expression qui allait être évaluée représente un problème de sécurité possible.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.jelly.js_interpolation.protect*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour atténuer les attaques d'exécution de code malveillant qui peuvent se produire à l'aide de Jelly Injection.
Valeur recommandée	vrai
Valeur par défaut	Faux
Cote de risque de sécurité	9
Impact fonctionnel	Cette propriété détermine au mieux si une expression est citée. Il peut citer à tort une expression légitime. Dans ce cas, il peut être nécessaire de marquer manuellement une expression comme étant sûre.
Risque de sécurité	(Modéré) L'injection JEXL est une forme d'injection d'entrée unique qui peut conduire à la fois à la falsification de requête intersite et à l'exécution ServiceNow AI Platform de code. La désactivation complète de la protection peut potentiellement ouvrir de nombreuses vulnérabilités de sécurité P1.
Solution de contournement	Pour marquer manuellement une expression comme sûre, ajoutez un préfixe SAFE à l'expression Jelly : `${SAFE :sysparm_input} ;` Ajouter aveuglément SAFE à chaque expression est une mauvaise façon d'aborder le problème, car cela peut ouvrir une vulnérabilité de sécurité. • N'ajoutez SAFE à une expression que si vous pouvez garantir que l'expression ne contient pas d'entrée du client. • Si c'est le cas, il est possible qu'un client malveillant provoque une évaluation du JavaScript privilégié.
Références	Balises Jelly Paramètres de sécurité élevée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la protection de l'interpolation Jelly JS pour les expressions imbriquées [Mis à jour dans Centre de sécurité 2.0]

Gérez la protection contre l'interpolation sur votre instance.

Utilisez cette propriété pour gérer la`glide.ui.jelly.js_interpolation.protect_nested_expressions` protection contre l'interpolation. La protection contre l'interpolation garantit que lorsque des expressions Jelly sont utilisées dans JavaScript, elles doivent être considérées comme sûres en entrant dans certaines catégories ou en étant marquées comme SAFE dans l'expression elle-même. Si cette atténuation n'est pas activée, un acteur malveillant peut envoyer un paramètre GET à une page Jelly et faire évaluer le contenu de ce paramètre en tant que JavaScript côté serveur avec des privilèges d'administrateur. Si cette propriété n'est pas définie sur la valeur conseillée **true**, les expressions Jelly malveillantes interpolées en JavaScript sont autorisées et un utilisateur peut exécuter du code à l'aide d'un modèle Jelly.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.jelly.js_interpolation.protect_nested_expressions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	Faux
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 9 • Score CVSS : critique • Détails du risque de sécurité : si la propriété est définie sur **faux**, les expressions Jelly malveillantes sont autorisées.
Dépendances et prérequis	Aucun

Renforcer les liens relatifs [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour appliquer des `glide.cms.catalog_uri_relative` liens relatifs à partir du paramètre URI sur /ess/catalog.do.

La `glide.cms.catalog_uri_relative` propriété applique les liens relatifs du paramètre URI sur /ess/catalog.do. Si `glide.cms.catalog_uri_relative` la valeur recommandée n'est pas définie sur true, l'URL n'est pas assainie avec la fonction enforceRelativeURL(url). Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le cadre d'un paramètre ou d'une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.cms.catalog_uri_relative*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour limiter les tentatives de liaison de contenu externe non autorisé.
Valeur recommandée	vrai
Valeur par défaut	Faux
Cote de risque de sécurité	2.6
Impact fonctionnel	Ce rattrapage applique la validation sur la page du catalogue de sorte que seules les URL relatives sont autorisées. Les liens existants vers des applications Web externes sont rompus.
Risque de sécurité	(Élevé) Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans le cadre d'un paramètre ou d'une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Appliquer la vérification de la liste d'autorisations d'URL [Mis à jour dans le Centre de sécurité 1.3, 1.5 et 2.0]

Utilisez la *glide.security.url.whitelist* propriété système pour ajouter une validation supplémentaire afin de vous assurer que toute URL externe introduite doit faire partie des URL sur liste d'inclusion.

Protégez vos utilisateurs contre la redirection ouverte côté client, qui permet aux attaquants de rediriger vos utilisateurs vers des pages non approuvées et malveillantes.

Si **glide.security.url.whitelist.strict_check** n'est pas défini sur la valeur recommandée **vrai**, toutes les URL externes sont autorisées à être redirigées tant que la propriété système **glide.security.url.whitelist** est vide. Si **glide.security.url.whitelist** n'est pas vide, seules les URL externes répertoriées dans cette propriété sont autorisées.

Définissez **glide.security.url.whitelist.strict_check** sur **vrai** ou assurez-vous que **glide.security.url.whitelist** est configuré avec les URL externes autorisées pour aider à sécuriser votre instance contre les attaques de redirection ouverte.

Cette propriété est applicable dans les cas suivants :

- /logout.do ?sysparm_goto_url={URL externe}
- /cms_login_redirect.do ?sysparm_goto_url={URL externe}

Après s'être déconnectés de l'instance, les utilisateurs sont dirigés vers un site de confiance externe :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- /logout_redirect.do ?sysparm_url={URL externe}
- /saml_redirector.do ?sysparm_uri={URL externe}

Lorsque SAML est activé, il invoque une URL de déconnexion du fournisseur d'identité (IdP).

Assurez-vous que la propriété *glide.security.url.whitelist.strict_check* est définie sur vrai ou *glide.security.url.whitelist* sur une valeur.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.security.url.whitelist*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour implémenter une redirection d'URL sécurisée lors de la connexion, de la déconnexion ou d'autres redirections. Cette propriété atténue l'une des 10 premières attaques OWASP appelée Redirections et transferts invalidés.
Type	Chaîne
Valeur par défaut	vrai
Valeur recommandée	vrai
Valeur	URL approuvées par votre organisation [un certain FQDN (nom de domaine complet) défini, ex. http://www.servicenow.com]
Cote de risque de sécurité	6.3
Impact fonctionnel	Ce rattrapage applique la validation sur la page de déconnexion. Elle peut avoir un impact fonctionnel sur l'utilisateur d'une instance avec une configuration SSO/SAML.
Risque de sécurité	(Élevé) La redirection ouverte côté client peut permettre à l'attaquant de rediriger les victimes/utilisateurs vers un site Web contrôlé par l'attaquant et est considérée comme un risque de sécurité.
Références	Erreurs et correctifs Multi-SSO (SAML 2.0)

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Formules Excel d'échappement [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour empêcher l'injection Excel, également connue sous le *glide.export.escape_formulas* nom d'injection de formule.

Empêchez l'exécution de formules potentiellement malveillantes dans des programmes tels qu'Excel après l'exportation et l'ouverture du fichier en échappant les formules dans ces fichiers. L'injection Excel se produit lorsque les sites Web intègrent des entrées non approuvées dans des fichiers Excel. Lorsque vous utilisez une application de feuille de calcul telle que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cellules commençant par +, -, = ou @ sont interprétées comme une formule à moins d'être correctement échappées. Les formules malveillantes présentent un risque même lorsque la feuille de calcul ne contient aucune information sensible, car elles peuvent être utilisées pour compromettre l'ordinateur du spectateur par l'exécution de code.

Définissez la propriété système **glide.export.escape_formulas** sur **vrai** pour échapper l'exécution de ces formules.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.export.escape_formulas*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour empêcher l'application contre Excel ou l'injection de formule.
Valeur recommandée	vrai
Valeur par défaut	Faux
Cote de risque de sécurité	6.4
Impact fonctionnel	Des formules malveillantes peuvent être utilisées pour détourner l'ordinateur de l'utilisateur en exploitant les vulnérabilités du tableur.
Risque de sécurité	(Modéré) Les formules malveillantes présentent un risque même lorsque la feuille de calcul d'intégration ne contient aucune information sensible, car elles peuvent être utilisées pour compromettre l'ordinateur du spectateur.
Solution de contournement	Comme alternative, envisagez de supprimer tous les espaces de fin dans la mesure du possible et de limiter toutes les données fournies par le client à des caractères alphanumériques.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

HTML d'échappement dans les vues de listes [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez cette propriété pour forcer les *glide.ui.escape_html_list_field* caractères d'échappement HTML pour les champs HTML d'une vue de liste.

Définissez *glide.ui.escape_html_list_field* la valeur **sur vrai** pour empêcher le rendu HTML dans les champs HTML de la vue de liste. Laisser le nettoyage HTML inactif à l'échelle de la plateforme (via la propriété système) ou par champ (via un attribut de schéma) peut entraîner des attaques de type XSS. Les attaques XSS peuvent permettre à un utilisateur ayant des privilèges faibles de détourner la session d'un utilisateur ayant des privilèges élevés ou d'interférer dans les comportements standard des applications Web, y compris les redirections ou les altérations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. C'est non réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_html_list_field*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour aider à prévenir les attaques de script de site à site des applications
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	3.1
Impact fonctionnel	Cette correction force l'encodage HTML à se produire sur l'interface utilisateur au niveau de l'analyseur HTML et rend ainsi les résultats encodés à l'utilisateur. Elle peut avoir un impact fonctionnel basé sur l'interaction de l'utilisateur de l'instance avec les données obtenues.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Échapper à JavaScript [mis à jour dans Centre de sécurité 1.3]

Utilisez cette propriété pour forcer l'échappement *glide.html.escape_script* des balises JavaScript (<script></script>) dans les champs HTML au cours des vues de listes.

La propriété *glide.html.escape_script* Glide permet de nettoyer les champs HTML. Si *glide.html.escape_script* cette option n'est pas définie sur la valeur conseillée true, les entrées ne seront pas nettoyées pour les champs HTML (codage de sortie) d'un contexte Java back-end en supprimant le JavaScript intégré. Javascript dans les champs HTML peut entraîner des XSS stockés et reflétés. La possibilité d'avoir un XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés tels que l'administrateur où un mouvement plus latéral peut être effectué.

Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.html.escape_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour empêcher les attaques de script de site à site contre une application.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette correction impose l'échappement de JavaScript dans l'interface utilisateur et rend les résultats encodés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité, en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Propriétés système disponibles Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Script Jelly d'échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Utilisez la propriété pour forcer l'échappement `glide.ui.escape_all_script` de tous les scripts injectés dans Jelly.

Cette propriété échappe à toutes les chaînes JS et HTML incluses dans <j :jelly> ... </j :jelly> avant qu'ils ne soient écrits dans le flux de sortie, ce qui évite que plusieurs problèmes XSS ne se produisent. Si `glide.ui.escape_all_script` n'est pas défini sur la valeur recommandée true, l'échappement des scripts injectés dans Jelly est désactivé. Sans cette atténuation, la plateforme devient largement ouverte à une variété d'attaques par injection de script. Un attaquant pourrait exécuter des scripts Rhino arbitraires sur l'instance.

⚠ Avertissement :
Soyez prudent lorsque vous utilisez ces balises. Si l'entrée de l'utilisateur est affichée ici, elle peut ouvrir une vulnérabilité de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_all_script*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Catégorie	Validation, nettoyage et codage
Objectif	Si la propriété n'est pas définie sur **vrai**, les développeurs doivent effectuer plusieurs étapes sur chaque script Jelly personnalisé pour éviter les problèmes XSS. Ces étapes incluent la localisation des variables Jelly envoyées au flux de sortie pour être rendues sur des pages Web, et l'exécution d'un échappement sur chacune des balises suivantes : $â {JS :expression} $â {HTML :expression} OU $â {JS,HTML :expression}
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	7.3
Impact fonctionnel	Cette correction applique l'échappement de Jelly au niveau de l'analyseur. Elle peut avoir un impact fonctionnel sur l'interaction de l'utilisateur avec les données résultantes.
Risque de sécurité	(Élevé) La validation des entrées doit s'effectuer sur toutes les entrées utilisateur saisies dans l'application. Ce faisant, les attaques par injection contre la plateforme peuvent être défendues et protégées.
Solution de contournement	L'interface utilisateur peut être affectée car certains scripts et balises HTML conçus pour le rendu sur une page Web peuvent sembler cassés. Cette correction envoie la page codée de sortie au navigateur pour restitution. Par exemple, au lieu de 'ma chaîne ici', il pourrait afficher '<u>ma chaîne ici</u> car la <u> balise a été correctement échappée. Dans ce cas, pour empêcher l'échappement, ajoutez le préfixe NOESC à l'expression Jelly pour empêcher l'échappement JS. Par exemple : • Devant : ($[jvar_context_menus]) ; • Après : ($[NOESC :jvar_context_menus]) ;

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Avant : $[jvar_ui_policy_scripts] • Après : $[NOESC :jvar_ui_policy_scripts] **⚠ Avertissement :** Soyez prudent lorsque vous utilisez ces balises. Si l'entrée de l'utilisateur est affichée ici, elle peut ouvrir une vulnérabilité de sécurité.
Références	Paramètres de sécurité élevée Balises Jelly

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Scripts d'échappement dans le bloc-notes [Mis à jour dans Centre de sécurité 1.3]

Découvrez comment le bloc-notes entre en ligne de compte dans la posture de sécurité de votre instance et comment le gérer afin que des scripts malveillants ne puissent pas y être exécutés.

Le bloc-notes est un moyen facile de définir des informations sur le serveur auxquelles vous pouvez accéder dans le navigateur. Un administrateur peut y faire figurer n'importe quoi, y compris des enregistrements arbitraires. Si cette propriété **n'est** pas définie sur la valeur recommandée true, il est possible d'exécuter des scripts malveillants comme une vulnérabilité de script de site à site.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.escape_scratchpad`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si la propriété n'est pas définie sur la valeur recommandée **vrai**, il est possible d'exécuter des scripts malveillants comme une vulnérabilité de script de site à site.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Workflow administration

Balisage XML d'échappement [Mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour forcer l'échappement *glide.ui.escape_text* des valeurs XML au niveau de l'analyseur avant de les transmettre au navigateur du client.

Le script de site à site se produit lorsqu'un attaquant injecte du JavaScript malveillant dans un point d'entrée. La plateforme/l'application ne parvient pas à échapper au JavaScript malveillant avant de le transmettre au navigateur de la victime pour exécution. Dans ce contexte, s'échapper signifie ce qui suit :

- **&** --> &
- **<** --> <
- **>** --> >
- **"** --> "
- **'** --> '
- **/** --> /

Exemple : <![CDATA[<script>alert('XSS Attack') ;]]>

Évasion : <script>alert('Attaque XSS') ; </script>

Assurez-vous que la propriété existe dans la table sys_properties et qu'elle *glide.ui.escape_text* est définie sur vrai.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_text*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	L'échappement XML garantit que les navigateurs n'analysent pas le JavaScript malveillant incorporé dans des données non approuvées et ne l'exécutent pas en tant que JavaScript. • Un utilisateur malveillant peut tenter une attaque XSS pour détourner la session d'autres utilisateurs ou rediriger l'utilisateur vers un site Web malveillant. • La Now Platform contient du code pour sécuriser les cookies, mais pour l'échapper, cette propriété doit être définie sur **vrai**.
Valeur recommandée	vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette correction applique le codage XML au niveau de l'analyseur XML sur l'interface utilisateur. Il restitue les résultats codés pour l'utilisateur, ce qui peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.

Solution de contournement	Une fois cette propriété définie sur **true**, l'affichage s'arrête sur les balises HTML dans la description de l'élément de catalogue ou dans le texte d'aide de la variable de l'élément de catalogue. Il se peut que vous ne puissiez pas utiliser le formatage HTML pour certains champs.
	
	Cependant, si la *glide.ui.escape_text* propriété est désactivée, toutes les expressions JEXL seront précédées d'un encodeur de sortie :
	
	`${JS :expression}`
	
	`${HTML :expression}`
	
	ou
	
	`${JS,HTML :expression}`

Échapper à la réponse XML

Gérez la façon dont les échappements XML sont gérés sur votre instance.

Utilisez cette propriété pour gérer si les réponses XML sont échappées. Si la propriété est définie sur la valeur recommandée **faux**, les réponses XML ne seront pas échappées, ce qui peut entraîner une attaque par injection XML. L'injection de contenu XML non intentionnel dans un message XML peut modifier la logique prévue d'une application.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.soaprequest.unescape_xml_response*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	Faux
Valeur par défaut	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **faux** désactive l'échappement XML, ce qui pourrait entraîner une attaque par injection XML.
Dépendances et prérequis	Aucun

Activer l'assainisseur HTML [mis à jour dans Centre de sécurité 1.3]

Utilisez la propriété pour activer l'include de script HTMLSanitizer, qui nettoie l'entrée HTML selon les attributs figurant sur la *glide.html.sanitize_all_fields* liste d'exclusion et la liste d'inclusion configurés dans un script.

Les types de champs disponibles avec le dictionnaire/les champs comprennent HTML et HTML traduit. Ces champs d'entrée HTML permettent aux utilisateurs d'écrire une entrée au format HTML, par exemple :

`<h1>Testez</h1>` en utilisant les balises HTML les plus basiques telles que `<img>`, `<a href ···>`et `<iframe>`.

Cela peut ouvrir la porte à un attaquant malveillant pour injecter un vecteur malveillant avec des balises HTML telles que :

`[<IMG SRC=" &#14; JavaScript:alert('XSS');">][],<IMG onmouseover="alert('xss')">[a href=" » onclick=alert(/xss/)]`.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.html.sanitize_all_fields*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêche l'application contre les attaques de script de site à site et d'injection HTML
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.8
Impact fonctionnel	Cette correction applique un mécanisme de codage de sortie HTML avant que les données utilisateur ne soient restituées à l'utilisateur. Si le client dispose d'une personnalisation qui implique le rendu de l'attribut HTML ou des données de contenu, il y a un impact sur la fonctionnalité.
Risque de sécurité	(Élevé) L'entrée de l'utilisateur doit être traitée en toute sécurité lorsque les données sont stockées et traitées sur l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Cela réduit les attaques de script de site à site côté client en encodant les données de sortie.
Solution de contournement	Cette propriété nettoie tous les champs HTML du système. Si vous devez activer l'assainissement HTML sur des champs individuels, consultez Activer l'assainissement sur des champs individuels. Vous pouvez également configurer la liste d'inclusion ou la liste d'exclusion pour nettoyer les attributs et les balises HTML conformément à la politique de votre organisation.
Références	Activation de l'assainisseur HTML Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les packages Java autorisés [Mis à jour dans Centre de sécurité 1.3]

La configuration de ces propriétés protège contre les API dangereuses exposées au moteur de scripting.

Configurez les tables système et installez le module d'extension recommandé en conséquence.

Si les valeurs de la `sys_whitelist_member` table et `sys_whitelist_package` ne sont pas vides, les API dangereuses peuvent être exposées au moteur de scripting. Les entrées correspondent à l'espace de noms Java qui n'a pas été approuvé par ServiceNow les équipes de sécurité.

Installez l'outil de suppression des appels de packages. Consultez Outil de suppression des appels de packages pour en savoir plus.

Contactez Service client et assistance pour modifier ces tables.

En savoir plus

Attribut	Description
Nom du module d'extension de la table	Tables: • `sys_whitelist_member` • `sys_whitelist_package` Module d'extension : com.glide.script.packages_call_removal
Type de configuration	Configuration tabulaire, Modules d'extension
Catégorie	Validation, nettoyage et codage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Protégez-vous des API dangereuses exposées au moteur de scripting.
Valeur recommandée	Vide
Valeur par défaut	Aucun. Il s'agit d'une configuration de table et non d'une propriété Glide, il n'y a donc pas de valeur par défaut.
Type de configuration	liste de tables, module d'extension
Risque de sécurité	(Élevé) Les API dangereuses peuvent être exposées au moteur de scripting. Ces API prises en charge introduiront probablement de l'instabilité et de l'insécurité au sein de l'instance.
Cote de risque de sécurité	8.2

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Outil de suppression des appels de packages

Activez et exécutez le module d'extension Outil de suppression des appels de packages (*com.glide.script.packages_call_removal*), puis décidez si chaque changement proposé doit être appliqué ou rejeté.

L'outil de suppression des appels de packages est un module d'extension qui :

- Analyse les scripts pour les appels de packages vers les ServiceNow AI Platform classes Java.
- Propose des changements pour les remplacer par les noms GlideScriptable préférés.
- Facilite les changements de script.

Remarque :
S'il s'agit d'un enregistrement du système de base, l'utilisation de la recommandation de l'outil entraîne le marquage de l'élément comme customer_update. Cependant, il peut toujours être utile d'utiliser cet outil car il marque les appels Packages,xxx.

L'outil de suppression des appels de packages peut signaler certains appels de package utilisés dans sa_mapping_ext_commands et sa_custom_operation. Ces appels de package appartiennent au Serveur MID. Comme il n'y a pas de classes, le code s'exécute dans Serveur MID. Si vous trouvez l'un des appels de package répertoriés suivants dans la section Erreurs, marquez-le comme Rejeté (Ignoré). L'outil ne signale plus cet appel de package.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content)` ;
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name)` ;
- `Packages.com.snc.sw.commands.HttpCallHandler` ;
- `Packages.com.snc.sw.dto.ProviderType.SSH`

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.script.packages_call_removal
Type de configuration	Définition du système > Modules d'extension

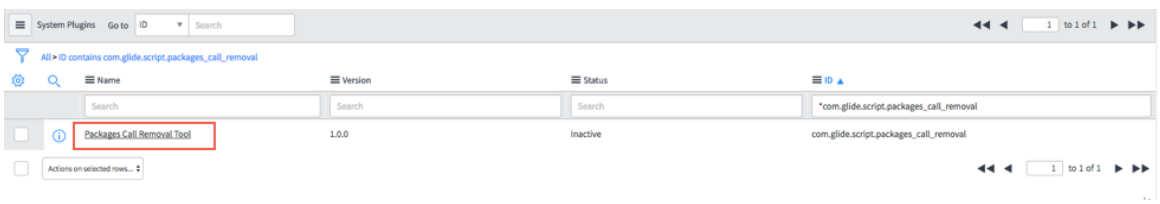
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

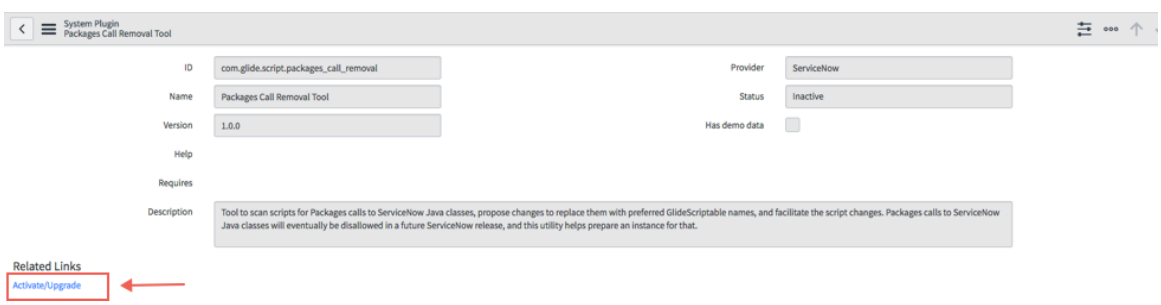
Attribut	Description
Objectif	Pour supprimer/remplacer les appels de package/membre non autorisés par des noms Glide acceptable (GlideScriptable) qui autorisent uniquement l'accès autorisé aux données.
Valeur recommandée	Actif
Impact fonctionnel	Cette correction remplacerait les appels de package par des API `GlideScriptable` et peut affecter les personnalisations qui incluent les appels de package. L'outil ne remplace pas automatiquement les appels de package. Au lieu de cela, il fournit des suggestions qui sont stockées dans la table packages_call_item. Votre administrateur peut ensuite décider d'accepter ou de rejeter la modification proposée.
Risque de sécurité	(Moyen) Les appels d'API côté client qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Ils doivent être validés pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes de configuration

1. Accédez à la **Définition du système** > **Modules d'extension**



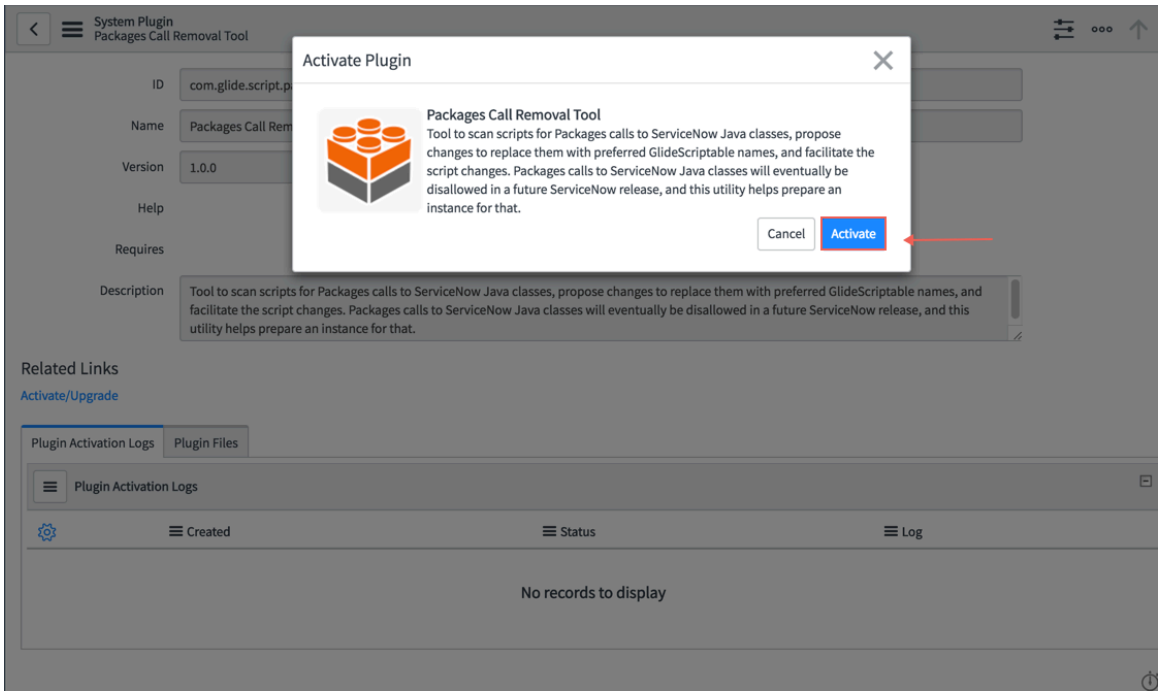
2. Rechercher l'ID du module d'extension = `com.glide.script.packages_call_removal`.



3. Cliquez sur **Activer/Mettre à niveau** pour activer le module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour vérifier les appels de package de liste d'inclusion et les appels aux membres de la liste d'inclusion, effectuez les actions décrites dans les sections Étapes de configuration de Restreindre les packages Java autorisés [Mis à jour dans Centre de sécurité 1.3].

Annuler le LDAP Nom unique initial [mis à jour dans Centre de sécurité 1.3 et supprimé dans la version 2.0]

Utilisez cette propriété pour gérer le nom unique d'un enregistrement de serveur LDAP.

Cette propriété contrôle le nom unique d'un enregistrement de serveur LDAP qui est inséré lors de l'exécution d'un script de correction prêt à l'emploi. Si elle est définie sur la valeur recommandée « » ou vide, les données du serveur LDAP peuvent être énumérées par un utilisateur possédant moins de privilèges.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ldap.initial.dn`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	vide
Valeur par défaut	vide
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : définir la valeur de la propriété sur « » ou vide peut rendre les données du serveur LDAP accessibles à un utilisateur avec des privilèges inférieurs.
Dépendances et prérequis	Aucun

Appliquer la sécurité stricte des cookies de session [Mis à jour dans Centre de sécurité 1.3]

Utilisez la `glide.ui.secure_cookies` propriété pour exiger des cookies correctement formatés

Lorsque vous définissez la propriété sur vrai, votre instance rejette une session si le cookie associé n'est pas au format attendu.

> **⚠ Avertissement :**
> Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.secure_cookies`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	8.8
Impact fonctionnel	Lorsque la propriété est définie sur vrai, les cookies mal formatés sont rejetés. Lorsqu'un tel cookie est rejeté, l'utilisateur doit se connecter à nouveau.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts [mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]

Utilisez la `glide.xmlutil.max_entity_expansion` propriété pour réduire la limite maximale d'expansion de l'entité.

Cette propriété contrôle la quantité maximale d'expansions d'entité dans un analyseur XML. Si `glide.xmlutil.max_entity_expansion` elle n'est pas définie sur la valeur conseillée de 3 000 ou moins, le script d'analyse GlideXMLUtil peut être vulnérable aux attaques par déni de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que la propriété *glide.xmlutil.max_entity_expansion* est définie sur 3 000 ou moins. Si l'instance est sur Washington ou une version ultérieure, la valeur implicite par défaut est 3 000 si l'enregistrement sys_properties n'existe pas. Si l'instance n'est pas sur Washington ou une version ultérieure, il est recommandé à l'administrateur de l'instance de créer un enregistrement de sys_properties avec le nom *glide.xmlutil.max_entity_expansion* et la valeur 3 000.

Remarque :
500 est le minimum par défaut imposé par le ServiceNow AI Platform, qui est considéré comme un seuil de sécurité.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.xmlutil.max_entity_expansion*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour se défendre contre les attaques d'expansion d'entité XML/Billion Laugh.
Valeur recommandée	3000
Valeur par défaut	100000
Cote de risque de sécurité	5.3
Impact fonctionnel	Si la personnalisation fait appel à l'expansion d'une grande entité, cela ServiceNow AI Platform peut bloquer tout traitement ultérieur.
Risque de sécurité	(Modéré) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources système.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Empêcher la création d'ACL vide [nouveau dans le centre de sécurité 2.0]

Définissez la *glide.security.empty_acl.popup_window.enabled* propriété sur la valeur sécurisée vrai pour bloquer les tentatives de création, de mise à jour ou d'enregistrement d'une ACL non valide. Ce paramètre fournit également un modèle côté client pour configurer un rôle ou un attribut de sécurité pour l'ACL.

La *glide.security.empty_acl.popup_window.enabled* propriété détermine si les utilisateurs qui effectuent des modifications basées sur des formulaires aux listes de contrôle d'accès (ACL), en particulier sys_security_acl, peuvent créer, mettre à jour ou enregistrer une ACL non valide qui a une condition de données, un script, un attribut de sécurité ou une liste de rôles non valide. Sinon, il reste non configuré (une ACL vide). À partir de la version, toute ACL vide refusera l'accès Xanadu . Dans ServiceNow les versions antérieures à Xanadu, une ACL vide autorise un accès inconditionnel.

Lorsque la *glide.security.empty_acl.popup_window.enabled* propriété est définie sur la valeur sécurisée true, elle bloque les tentatives de création, de mise à jour ou d'enregistrement d'une ACL non valide ou vide, et fournit un modèle côté client pour configurer un rôle ou un attribut de sécurité pour l'ACL. Si la propriété est définie sur la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

valeur non sécurisée faux, ces tentatives seront autorisées et aucun modèle côté client ne sera affiché.

Remarque : cette propriété est sensible à la casse. Par exemple, une valeur Vrai (T majuscule) sera évaluée comme fausse. De plus, cette propriété ne fonctionne que lorsque le module d'extension de haute sécurité (com.glide.high_security) est installé et actif.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.empty_acl.popup_window.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété est définie sur vrai, la fenêtre contextuelle d'avertissement d'ACL vide empêchera l'utilisateur de soumettre une ACL vide côté client. Si elle est définie sur faux, la fenêtre contextuelle ne s'affiche plus.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété permet à l'utilisateur d'activer et de désactiver la fenêtre contextuelle d'avertissement ACL vide.
Références	Empêcher la création d'ACL vide [nouveau dans le centre de sécurité 2.0]

Définir les types MIME téléchargeables restreints [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]

Utilisez la propriété pour télécharger des `glide.ui.attachment.force_download_all_mime_types` types MIME et non pour les afficher en ligne dans le navigateur.

Si `glide.ui.attachment.download_mime_types` elle inclut des types MIME dangereux tels que text/html, image/svg, image/svg+xml, application/xml, les fichiers dangereux peuvent être affichés en ligne dans le navigateur, ce qui peut entraîner des attaques de script de site à site (XSS). Cette propriété correspond à la liste des types MIME de pièce jointe séparés par des virgules, qui ne s'afficheront pas en ligne dans le navigateur. Par exemple, l'inclusion de texte/html force le téléchargement des fichiers HTML vers le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur. La tenue à jour de cette liste empêche les attaques de script de site à site.

Si la `glide.ui.attachment.download_mime_types` propriété système n'inclut pas de types MIME dangereux tels que « text/html, image/svg,image/svg+xml,application/xml »,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les fichiers dangereux peuvent être affichés en ligne dans le navigateur. Cela peut entraîner des attaques de script de site à site (XSS). Cette vérification n'est pertinente que lorsque `glide.ui.attachment.force_download_all_mime_types` cette option est définie sur **faux**.

Cette propriété est une liste de types MIME de pièce jointe séparés par des virgules, qui ne sont pas alignés dans le navigateur. Par exemple, l'inclusion de texte/html force le téléchargement des fichiers HTML vers le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur.

Si `glide.ui.attachment.force_download_all_mime_types` la valeur est définie sur **faux**, vérifiez que la `glide.ui.attachment.download_mime_types` propriété système inclut les types MIME dangereux text/html,image/svg,image/svg+xml,application/xml.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.attachment.force_download_all_mime_types`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Chaîne (liste de types MIME séparés par des virgules)
Valeur recommandée	text/html,image/svg,image/svg+xml,application/xml
Valeur par défaut	text/html,image/svg,image/svg+xml,application/xml
Valeur de secours	text/html,image/svg,image/svg+xml,application/xml
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Risque de sécurité : la tenue à jour correcte de cette liste permet d'éviter les attaques de script de site à site.
Dépendances et prérequis	Cette vérification n'est pertinente que lorsque `glide.ui.attachment.force_download_all_mime_types` sa valeur est définie sur **faux** ou qu'elle n'existe pas dans la table Propriétés système [sys_properties].

Restreindre les types MIME chargés [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Utilisez la propriété pour activer la vérification du type MIME pour les `glide.security.file.mime_type.validation` téléchargements. Vous pouvez activer (définir la propriété sur **true**) ou désactiver (définir la propriété sur **false**) pour les pièces jointes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` .
Le type MIME est vérifié uniquement pour les extensions spécifiées `glide.attachment.extensions` lors du chargement. Pour en savoir plus, consultez Restrict file extensions .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que la propriété `glide.ui.jelly.js_interpolation.protect_nested_expressions` Glide existe et qu'elle est définie sur la valeur vrai. Si la propriété n'apparaît pas dans la table sys_properties, ajoutez un nouvel enregistrement.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.file.mime_type.validation`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour appliquer la vérification du type MIME / des octets magiques pendant les téléchargements de fichiers.
Valeur recommandée	vrai
Valeur par défaut	vrai
Cote de risque de sécurité	5.4
Impact fonctionnel	Cette correction permet la vérification de type MIME sur les pièces jointes à l'application. Aucun impact sur la fonctionnalité, sauf s'il y a une intention malveillante dans le chargement des fichiers, car cette validation vérifie simplement la mauvaise synchronisation entre le type MIME et les données.
Risque de sécurité	(Moyen) Pour réduire les vulnérabilités telles que l'inclusion de fichiers et les chargements de fichiers malveillants, la vérification du type MIME doit être activée.
Références	Administering attachments

Voir Paramètres de sécurisation renforcée pour plus de détails sur la configuration des propriétés de sécurisation renforcée.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]

Assurez-vous que les propriétés ET `glide.xml.entity.whitelist.enabled` sont définies sur les valeurs recommandées pour éviter les attaques d'entités `glide.xml.entity.whitelist` externes XML (XXE).

Protégez-vous contre les attaques XXE en utilisant une liste d'autorisation pour empêcher les attaquants d'inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait entraîner des attaques supplémentaires utilisant la relation de confiance du serveur avec d'autres entités.

Ajoutez `http://java.sun.com/j2ee/dtds/` à la valeur de la propriété système **glide.xml.entity.whitelist** , puis définissez la propriété système **glide.xml.entity.whitelist.enabled** sur **true**.

Des valeurs autres que `http://java.sun.com/j2ee/dtds/` peuvent être incluses dans la propriété **glide.xml.entity.whitelist** , mais ne sont pas nécessaires pour l'état de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plateforme prête à l'emploi. Examinez toutes les valeurs supplémentaires pour déterminer si elles sont sûres.

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.xml.entity.whitelist,glide.xml.entity.whitelist.ena`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de remédiation doit être activé pour se défendre contre les attaques XXE.
Valeur recommandée	http://java.sun.com/j2ee/dtds/
Valeur par défaut	http://java.sun.com/j2ee/dtds/
Cote de risque de sécurité	9.8
Impact fonctionnel	Si la personnalisation utilise une entité externe, et non une inclusion répertoriée dans la `glide.xml.entity.whitelist` propriété, NOW Platform peut bloquer tout traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser la DTD pour inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait conduire à d'autres attaques utilisant la relation de confiance du serveur avec d'autres entités.

Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mis à jour dans Centre de sécurité 1.3]

Si les personnalisations ne nécessitent pas l'expansion de l'entité, utilisez la propriété pour désactiver complètement l'expansion de l'entité `glide.xmlutil.max_entity_expansion` externe. Le code XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

Si la propriété `glide.stax.whitelist_enabled` Glide n'existe pas dans la table Propriétés système [sys_properties] ou n'est pas définie sur la valeur recommandée **vrai**, toutes les entités externes sont autorisées lorsque la propriété `glide.stax.allow_entity_resolution` Glide est définie sur la valeur **vrai**.

Si les personnalisations ne nécessitent pas d'expansion d'entité, utilisez la propriété pour désactiver complètement l'expansion d'entité `glide.stax.allow_entity_resolution` externe. Le code XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

- Si vous définissez `glide.stax.allow_entity_resolution` la valeur **sur vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, en fonction du paramètre de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez `glide.stax.allow_entity_resolution` la valeur **sur faux**, toute la résolution et l'expansion de l'entité sont bloquées. Pour en savoir plus sur cette propriété, reportez-vous à la section Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [Mis à jour dans Centre de sécurité 1.5].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque **glide.stax.whitelist_enabled** est défini sur **vrai**, définissez une liste de FQDN délimités par des virgules dans la propriété **glide.xml.entity.whitelist** , qui sont les seules URL pouvant être atteintes à l'aide de la propriété de traitement d'entité XML. Pour en savoir plus, consultez Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0]. Les attaquants peuvent utiliser cette vulnérabilité pour étendre les données de manière exponentielle dans une attaque d'expansion d'entités externes (XXE), consommant rapidement toutes les ressources système.

Prérequis

Avant de définir cette propriété :

- Définissez les propriétés et `glide.xml.entity.whitelist.enabledglide.stax.whitelist_enabled` sur **vrai**. Pour en savoir plus, consultez Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0].
- Définissez une liste de FQDN délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL pouvant être atteintes à l'aide de la propriété de traitement de l'entité XML. Pour en savoir plus, consultez Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0].

⚠ Avertissement :
Il s'agit d'une propriété de la sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.stax.whitelist_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour se défendre contre une attaque XML Entity Expansion/Billion Laugh.
Valeur recommandée	vrai
Valeur par défaut	Faux
Cote de risque de sécurité	9.8
Impact fonctionnel	Si la personnalisation utilise l'expansion de l'entité, elle ServiceNow AI Platform peut bloquer tout traitement ultérieur.
Risque de sécurité	Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle dans une attaque d'expansion d'entités externes (XXE), consommant rapidement toutes les ressources système.
Solution de contournement	Si la personnalisation nécessite le développement de l'entité, définissez cette propriété sur true et suivez les étapes décrites à la rubrique Restreindre les entités externes XML [Mis à jour dans Security Center 1.3 et 2.0].

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Nettoyer tous les champs HTML traduits [nouveau dans Security Center 2.0]

Découvrez comment configurer la *glide.translated_html.sanitize_all_fields* propriété sur la valeur sécurisée pour vous assurer que tous les *translated_html* éléments sont assainis avec un assainisseur HTML.

Lorsque la *glide.translated_html.sanitize_all_fields* propriété est définie sur vrai, tous les *translated_html* éléments sont nettoyés avec un assainisseur HTML. Si la propriété est définie sur false, seuls les éléments dont l'attribut *html_sanitize* de dictionnaire est défini sur true seront nettoyés. Cet assainissement permet d'empêcher les attaquants d'intégrer du contenu malveillant susceptible de conduire à des attaques de script de site à site (XSS).

En savoir plus

Attribut	Description
Nom de la configuration	*glide.translated_html.sanitize_all_fields*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 4,6 • Score CVSS : moyen • Détails du risque de sécurité : ne pas configurer cette propriété sur la valeur sécurisée vrai n'assainit pas tous les éléments HTML, ce qui augmente la probabilité qu'un acteur malveillant intègre du contenu malveillant dans un champ.
Dépendances et prérequis	Aucun
Impact fonctionnel	Permet aux clients d'accéder à n'importe quelle information de table si le widget est défini sur public et inclus dans la valeur de la propriété.

Nettoyer le HTML dans les champs de description du module de l'espace de travail Impact [Nouveau dans Security Center 7.0]

Nettoyez le code HTML dans les champs de description en supprimant les balises HTML qui sont des sources d'attaques par injection HTML avec la *sn_impact_common.blacklist_tags_HTML_injection* propriété.

Le module Impact Workspace autorise le HTML dans les champs de description suivants :

- Champ customer_notes des tables sn_impact_common_capabilities_map et sn_impact_common_par_version_phase_app_mapping.
- Champ manual_description de la table sn_impact_common_manual_capability_description.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque cette propriété système contient une liste de balises HTML séparées par des virgules (par exemple, des scripts), ces balises et leur contenu sont supprimés des parties HTML des champs répertoriés. La suppression de ces balises permet de nettoyer le HTML dans les champs de description en supprimant les balises HTML qui sont des sources d'attaques par injection HTML. Si cette propriété n'est pas définie dans la table Propriétés système [sys_properties], la valeur par défaut est une liste de balises HTML refusées. Si la propriété est vide, toutes les balises HTML sont autorisées.

Utilisez l'option *sn_impact_common.blacklist_tags_HTML_injection* fournir une liste séparée par des virgules de balises HTML qui sont supprimées des champs de description du module Espace de travail d'impact. Cette suppression permet d'éviter les attaques par injection HTML. Au minimum, cette liste doit contenir le contenu de la liste par défaut. Si la propriété n'est pas définie dans la table Propriétés système [sys_properties], elle utilise par défaut le script de liste,iframe,object,embed,form,onerror,onload,style,img,video,audio,source,button.

En savoir plus

Attribut	Description
Nom de la propriété	*sn_impact_common.blacklist_tags_HTML_injection*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Nettoyez le code HTML dans les champs de description en supprimant les balises HTML qui sont des sources d'attaques par injection HTML.
Valeur recommandée	Au minimum, la valeur par défaut de script,iframe,object,embed,form,onerror,onload,style,img,video,audio,sourc
Valeur par défaut	script,iframe,object,embed,form,onerror,onload,style,img,video,audio,sourc
Cote de risque de sécurité	4.4
Impact fonctionnel	Si une balise HTML est ajoutée à la liste par défaut, elle peut limiter la fonctionnalité HTML requise des champs de description. L'impact exact dépend de l'instance client.
Risque de sécurité	(Moyen)
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Définir une politique de sécurité de contenu sûre pour les fichiers SVG [Nouveau dans Security Center 1.3]

La *com.glide.csp.self_script_src_svg* propriété ajoute la directive **script-src none** à l'en-tête HTTP Content-Security-Policy lorsque vous accédez aux SVG (Scalable Vector Graphics) via l'extension de fichier IIX (Translation Memory Index).

La *com.glide.csp.self_script_src_svg* propriété empêche l'exécution de pièces jointes malveillantes qui stockent des attaques de script de site à site (XSS) dans une instance. Sans cette politique, un acteur malveillant pourrait amener un utilisateur à exécuter du code

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

JavaScript arbitraire dans son navigateur Web, ce qui pourrait entraîner des vulnérabilités de sécurité telles que l'exfiltration de données et la prise de contrôle de session.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.csp.self_script_src_svg`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	vrai
Valeur par défaut	vrai
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée vrai peut amener un utilisateur à exécuter du code JavaScript arbitraire à partir d'un acteur malveillant.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété empêche les fichiers SVG (Scalable Vector Graphics) d'accéder à des scripts externes.

Service d'exportation de journal (LES)

Service d'exportation de journal (LES) vous permet d'exporter de manière transparente vos journaux système d'instance et d'application vers vos outils d'analyse de la sécurité de l'entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

Explorer



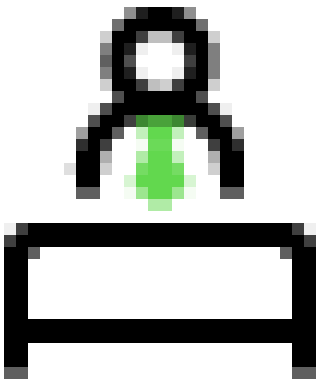
En savoir plus sur le service d’exportation de grumes (LES)

Configurer



Configurer LES pour les consommateurs Kafka et MID Server

Administrer



Administration des ERP

Utiliser



Examiner les rapports de journal à l’aide du LES

Référence



En savoir plus sur diverses informations sur l’application

Dépannage et demande d'aide

- Poser des questions ou y répondre Service d'exportation de journal (ERP) dans le ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Pour les recommandations de clonage pour les LES, y compris les tables à conserver et à exclure, consultez Tables à conserver pour conserver la configuration LES .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration Service d'exportation de journal (LES)

Le service LES offre une intégration hautement évolutive et en temps quasi réel avec vos outils d'analyse, qui est facile à configurer et à gérer. Si vous débutez avec LES, lisez cette section de présentation pour savoir ce que l'outil peut faire.

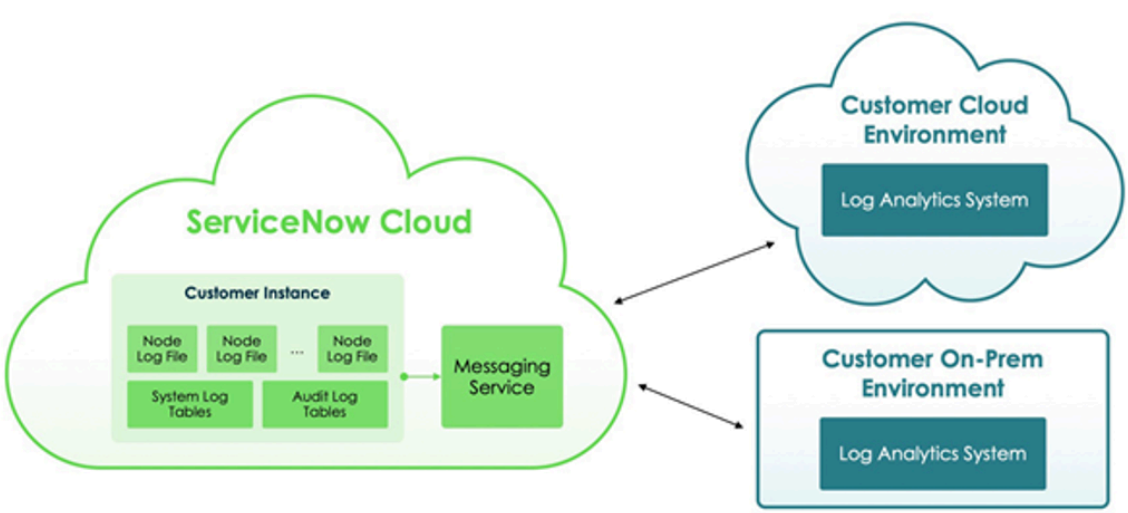
Vérifiez vos droits pour déterminer si vous avez accès à .Service d'exportation de journal

Vue d'ensemble de Service d'exportation de journal

L'outil d'intégration vous permet d'exploiter vos solutions analytiques pour effectuer les opérations suivantes :

- Détecter ServiceNow les menaces de sécurité et analyser les incidents de sécurité
- Dépannage et optimisation ServiceNow des performances de l'application
- Surveiller et optimiser ServiceNow l'expérience utilisateur

Le LES exploite une ServiceNow AI Platform capacité appelée Service de messagerie Hermes, qui est un service Apache Kafka de transport et de mise en file d'attente multilocataires, multiclusters, qui permet à votre instance de produire et de consommer de grands volumes d'événements Kafka. Apache Kafka est une plateforme de streaming de données open source qui fournit un point d'intégration unique pour l'échange de données entre les systèmes business de votre organisation.



Le LES transmet une copie des événements du journal au fur et à mesure de leur génération au Service de messagerie Hermes.

Il s'agit Service de messagerie Hermes d'un service de transport de données et de mise en file d'attente multilocataire, multicluster, qui Apache Kafka permet à votre instance de produire et de consommer de gros volumes d'événements Kafka. Il Service de messagerie Hermes s'agit d'une ServiceNow AI Platform aptitude disponible dans le cadre de Connexion au flux, Service d'exportation de journal (LES) et Réplication de données d'instance (IDR).

Les systèmes d'analyse de journal externes, dans le cloud ou sur site, peuvent utiliser et consommer les événements de journal à partir du Service de messagerie Hermes. Le LES offre trois options de connectivité pour consommer les journaux :

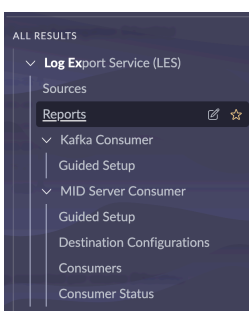
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dédié Serveur MID: un dédié Serveur MID est installé sur site ou dans le cloud qui se connecte automatiquement à Service de messagerie Hermes des événements de journal en continu, puis les pousse vers des outils d'analyse de journal via une connexion REST.
- Tirer parti du connecteur Kafka de votre solution d'analyse de journaux (par exemple, Splunk) : un connecteur Kafka provenant du produit d'analyse de journaux de votre choix est installé sur site ou dans le cloud qui se connecte automatiquement à Service de messagerie Hermes, extrait en continu les événements de journal et les transmet ensuite aux outils d'analyse de journaux.
- Directement à partir de votre système Kafka : votre système Kafka se connecte directement à et Service de messagerie Hermes utilise ses commandes et sa connectivité natives du protocole Kafka pour extraire les événements des journaux.

Remarque :
Si votre message Kafka dépasse la mémoire tampon configurée, Hermes peut renvoyer une erreur indiquant qu'il est plus grand que la mémoire tampon totale que vous avez configurée.

Pour configurer et gérer LES, vous devez l'installer à partir de ServiceNow Store. L'application LES propose des configurations guidées pour vous aider à installer le service, des pages pour configurer le service (sources de journal, consommateurs et destinations) et des rapports pour comprendre la création et la consommation de journaux.



Remarque :
vous pouvez également créer une nouvelle configuration source. Consultez Créer une configuration de source de journal pour plus d'informations.

Service d'exportation de journal utilisateurs

Service d'exportation de journal a les utilisateurs suivants.

Utilisateurs	Description
Administrateur d'application [sn_logstoanalytics.admin]	Ce rôle est installé en même temps que l'application LES et permet à un non-administrateur d'utiliser l'application.
Administrateur système [administrateur]	Le rôle administrateur est requis pour la configuration de l'application du magasin LES.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Service d'exportation de journal avantages

Avantage	Fonctionnalité	Utilisateurs
Créer une configuration de la source du journal pour définir des filtres sur les journaux	Créer une configuration de source de journal	Administration d'application
Configuration guidée de l'expérience pour les consommateurs Kafka	Configuration guidée pour les consommateurs Kafka	Administrateur système
Configuration guidée de l'expérience pour les consommateurs de Serveur MID	Configuration guidée pour les consommateurs de Serveur MID	Administrateur système
Examinez le tableau de bord des rapports de journal pour analyser la taille de chaque journal de données	Examiner le rapport du journal	Administrateur système ou administrateur d'application

Ce qu'il faut explorer ensuite

Pour en savoir plus sur l'utilisation Service d'exportation de journal, consultez :

- Administration (Service d'exportation de journal ERP)
- Configuration Service d'exportation de journal (LES)
- Utilisation (Service d'exportation de journal LES)
- Service d'exportation de journal Références (LES)

Sources du journal

Service d'exportation de journal (LES) peut exporter des sources de journal à partir de certaines tables de journal système, de la table d'audit et des fichiers journaux de nœud d'application.

Voici les sources de journal qui peuvent être exportées par les LES.

- Tables de journaux système
  - table syslog : affichez les avertissements et les erreurs pour les processus, les enregistrements et les événements non critiques de l'instance, tels que l'utilisation de la mémoire sur le serveur
  - Table syslog_transaction : afficher toute l'activité du navigateur pour une instance
  - sys_outbound_http_log table : affichez toutes les demandes et réponses pour les services Web sortants tels que REST et SOAP
- Table d'audit : utilisez la table sys_audit afficher les changements apportés à l'enregistrement des tables choisies pour l'audit
- Fichiers journaux de nœud d'application : utilisez les fichiers journaux localhost pour afficher les erreurs de nœud d'application. Votre instance aura plusieurs nœuds et chaque nœud aura plusieurs fichiers journaux.

Reportez-vous à la section Journaux système pour en savoir plus sur le schéma et l'objectif des sources de journal ci-dessus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administration (Service d'exportation de journal ERP)

Utilisez LES pour créer une configuration de source de journal et des rubriques multiples pour chaque type de source.

Créer une configuration de source de journal

Réglez et définissez des filtres sur les journaux à transmettre en créant une configuration de source de journal.

Avant de commencer

Rôle requis : admin ou sn_logstoanalytics.admin

Procédure

1. Accédez à la **Tous** > **Service d'exportation de journaux**.
   Une liste des configurations sources s'affiche.
2. Sélectionnez **Nouveau** si vous souhaitez créer une configuration source.
   Vous pouvez également sélectionner une configuration source existante si vous souhaitez la modifier.
   Le formulaire Source s'affiche.
3. Renseignez les champs du formulaire.

Formulaire source

Champs	Description
Type de source	Types de sources de journal ○ Journal de nœud ○ Table Consultez Sources du journal pour plus d'informations.
Niveau de journal	Un ensemble de niveaux de journalisation standard qui peuvent être utilisés pour contrôler la sortie de journalisation. Conformément à la convention, chaque niveau transmettra des journaux de gravité égale ou supérieure. **Remarque :** Ce champ n'est visible que lorsque l'une des conditions suivantes est remplie. ○ Lorsque vous sélectionnez Journal de nœud comme type de source ○ Lorsque vous sélectionnez Table comme type de source et que la table est syslog
Accepte	Spécifie le format dans lequel les journaux sont transmis à Hermes. Ils peuvent être envoyés au format JSON ou au format texte brut.
Table	Sélection de table pour les journaux de type table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	Remarque : Ce champ n'est visible que lorsque vous sélectionnez Table comme type de source.
Type de filtre	Conditions pour transférer les journaux de manière sélective. **Remarque :** Ce champ n'est visible que si vous sélectionnez syslog ou sys_audit comme table.

4. Passez en revue les détails de la liste connexe Rubriques sources.
   Vous pouvez examiner chacune des tables de journal et créer ses propres rubriques.

   Remarque : La liste connexe n'est visible que si vous sélectionnez Table de journaux dans le champ Type de filtre.

   Le nom de la rubrique n'est pas renseigné automatiquement et vous pouvez sélectionner ou créer ses propres rubriques.

5. Sélectionnez une rubrique pour la table de journal.

   Vous pouvez sélectionner une rubrique existante ou créer une nouvelle rubrique pour une table de journal.

   a. Sélectionnez **Nouveau** pour créer une rubrique source pour une table de journal. Le formulaire Rubriques sources s'affiche.
   b. Sélectionnez la table requise dans le champ Table de journal.
   c. Sélectionnez l'icône de recherche dans le champ Rubrique.

      Remarque : Vous pouvez sélectionner une rubrique existante dans la liste. Vous pouvez également créer une nouvelle rubrique en sélectionnant **Nouveau** dans la liste Rubriques Kafka. Reportez-vous à la section Créer un type source et des rubriques multiples dans la table source LES pour créer une rubrique Kafka.

   d. Sélectionnez **Soumettre** dans le formulaire Rubriques sources.

6. Affichez la table de journal récemment créée et sa rubrique correspondante dans la liste connexe Rubriques sources.
7. Sélectionnez **Soumettre** pour créer une configuration source.

Créer un type source et des rubriques multiples dans la table source LES

Utilisez les journaux pour chaque type de source en créant plusieurs rubriques par type de source. Vous pouvez désormais tirer parti de l'option de sélection personnalisée de rubriques spécifiques pour différentes sources de journal pendant le processus de débogage, sans impact sur les autres tables de journal.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remarque :
Si vous supprimez une source de journal, la rubrique correspondante de la table sys_kafka_topic n'est pas supprimée. Si vous créez à nouveau la source de journal, la rubrique existante peut être réutilisée, ce qui garantit la continuité et évite la recréation inutile de rubriques.

Rôle requis : admin ou sn_logstoanalytics.admin

Procédure

1. Accédez à la **Tous** > **Service d'exportation de journaux (LES)** > **Sources**.
2. Cliquez sur **Nouveau** pour créer une nouvelle source.
   Le formulaire Source s'affiche. Auparavant, le champ **Rubrique** était renseigné automatiquement une fois le **type de source** sélectionné. À partir de Yokohama, chaque type de source peut créer sa propre rubrique. Il n'est pas renseigné par défaut lors de la sélection du **type de source** ou du nom de **table** . Ils peuvent être créés soit directement à partir des rubriques Kafka, soit à partir du champ de référence.

   Remarque :
   Étant donné que sys_audit table comporte plusieurs tables de journal, aucune rubrique spécifique n'est affichée dans la colonne Rubrique de la liste Sources. Auparavant, tous les types de sources avaient la même rubrique. Vous pouvez maintenant sélectionner différentes rubriques pour différentes sources.

3. Sélectionnez l'icône de recherche pour accéder à la liste des rubriques Kafka.
   La liste des sujets Kafka s'affiche.
4. **Facultatif :** Créez la nouvelle rubrique Kafka en suivant les étapes suivantes.

   Remarque :
   Cette étape s'applique uniquement si vous souhaitez créer une nouvelle rubrique pour un type de source sélectionné.

   a. Sélectionnez **Nouveau** pour créer une rubrique Kafka pour le type de source sélectionné. Le formulaire de rubrique Kafka s'affiche.
   b. Renseignez les champs du formulaire.

   Formulaire source

Champs	Description
Nom	Nom de la rubrique que vous créez
ID d'application	Entrer sn_logstoanalytics
Espace de noms	Entrer l'espace de noms par défaut
Partition	Le champ de partition d'une rubrique dans Hermes fait référence aux partitions dans lesquelles les données de la rubrique sont divisées. Elle joue un rôle clé dans l'évolutivité et le parallélisme

   c. Sélectionnez **Soumettre** pour créer la nouvelle rubrique Kafka.
5. Sélectionnez le **type de source** que vous souhaitez créer pour une rubrique particulière.
6. Sélectionnez la rubrique requise dans la liste pour le **type de source** sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Soumettre** pour créer le type de source avec les sélections particulières.
   Le type de source s'affiche dans la liste Sources avec le nom de la rubrique sélectionnée et d'autres informations.

Configuration Service d'exportation de journal (LES)

Utilisez la configuration guidée pour passer par la configuration initiale du LES. La configuration guidée vous aide à planifier le déploiement du produit et à effectuer la configuration de base pour la mise en service.

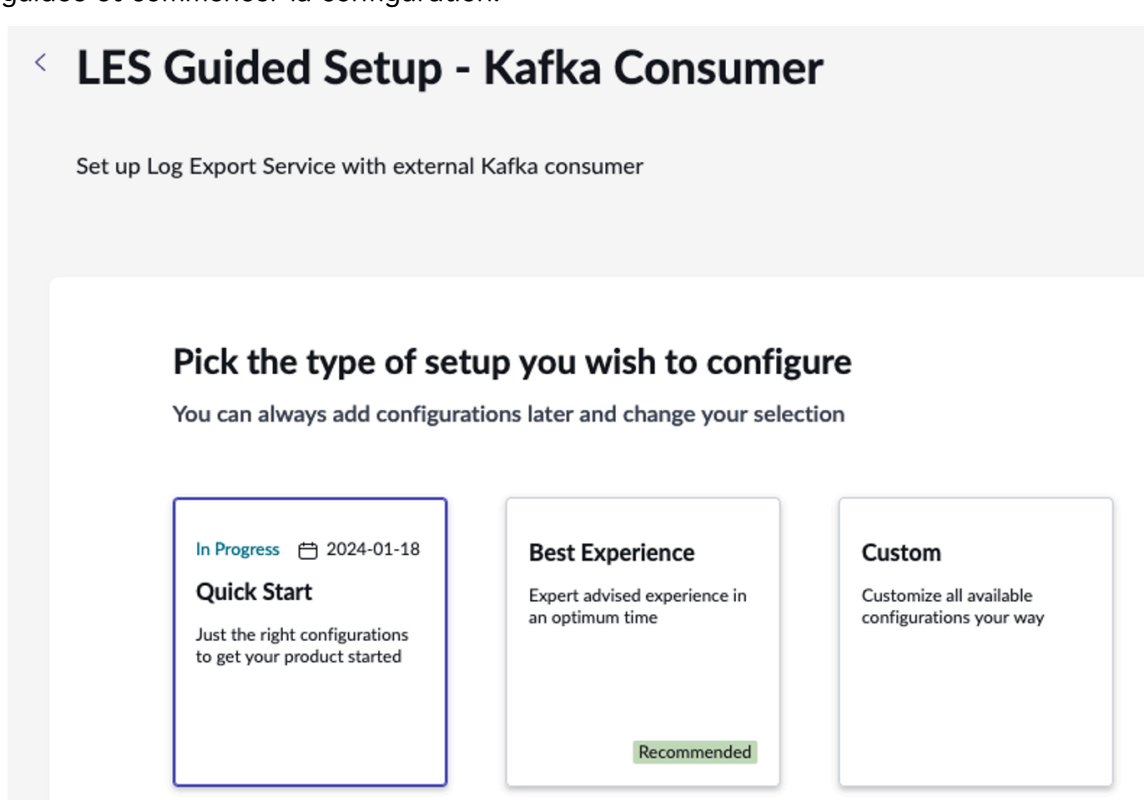
La configuration guidée organise les activités de configuration en catégories. Chaque catégorie fournit des informations, telles que des conseils de planification, des étapes de pré-configuration et des liens d'accès à des contenus d'aide utiles. Les catégories fournissent également un ensemble de liens vers les pages de votre instance où vous effectuez la configuration. Le processus de configuration guidée garde une trace de ce que vous avez terminé, de sorte que vous pouvez arrêter et reprendre là où vous vous étiez arrêté.

Consommateur Kafka

Utilisez la configuration guidée pour passer par la configuration initiale de LES pour les consommateurs Kafka.

Page d'accueil de la configuration guidée

La page d'accueil de la configuration guidée contient une vue d'ensemble des types de configuration pour votre configuration guidée. Vous pouvez sélectionner votre type de configuration guidée, puis **sélectionner Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.



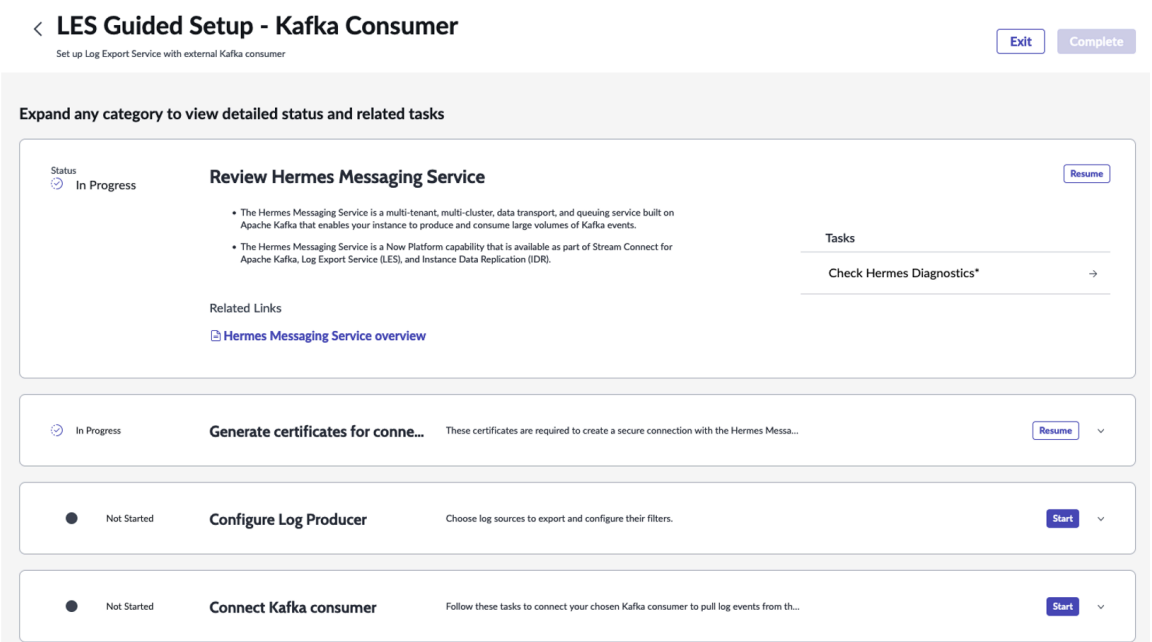
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les trois configurations de cette page, Démarrage rapide/Meilleure expérience/Personnalisé, fournissent les mêmes tâches et fonctionnalités. Il est nécessaire de coordonner l'intégration entre l'instance ServiceNow et l'outil d'analyse du journal de destination avec l'administrateur respectif. L'administrateur de l'analyse du journal doit configurer son outil pour se connecter à l'instance ServiceNow en toute sécurité. Il est recommandé de partager le document avec l'administrateur de l'analyse Set up a secure connection to the Hermes Messaging Service du journal à l'avance. Même si vous avez marqué une tâche comme terminée, vous pouvez revenir en arrière et la décocher à nouveau en cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la case **Modifier** pour la tâche que vous souhaitez décocher. La case **Marquer comme terminé** ne sera plus cochée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et des descriptions des catégories et des tâches associées. Vous pouvez cliquer sur la flèche du menu déroulant pour afficher des informations sur la catégorie ou sur le bouton Démarrer pour ouvrir les étapes de la configuration guidée et commencer la configuration.



Effectuez les tâches de chaque catégorie en suivant les instructions de configuration.

Configuration guidée pour les consommateurs Kafka

Implémentez les étapes suivantes pour une configuration guidée complète pour les consommateurs Kafka.

Avant de commencer

Accédez à la **Service d'exportation de journaux (LES)** > **Consommateur Kafka** > **Configuration guidée**. Sélectionnez le type de configuration que vous souhaitez configurer, puis sélectionnez **Continuer**.

Remarque :
Lors de l'installation de l'application Service d'exportation de journal , ServiceNow met en service l'infrastructure sous-jacente Service de messagerie Hermes . Sachez que ce processus peut prendre jusqu'à quelques heures à partir du moment où vous demandez l'installation de l'application Service d'exportation de journal .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : admin

Procédure

1. Passez en revue Service de messagerie Hermes les diagnostics.

   Nous vous recommandons de vérifier que l'outil Service de messagerie Hermes de diagnostic est en cours d'exécution, qui s'affiche à l'écran Hermes pendant cette étape. Si vous voyez une erreur « Page introuvable » sur cette page, Hermes elle n'est pas installée et vous devez contacter votre administrateur système.

   - Informations sur la Service de messagerie Hermes configuration : Les informations d'amorce suivantes sont utilisées pour se connecter au . Le « Starter Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et « Consumer Bootstrap 1 & 2 » sont utilisés pour récupérer des messages à partir de Hermes.
     - Amorce du créateur
     - Amorce de consommateur 1
     - Amorce de consommateur 2
   - PKI d'instance : le composant d'infrastructure de clé publique d'instance (PKI) permet à une instance ServiceNow d'agir en tant qu'émetteur dans une hiérarchie de confiance X.509.
   - Connectivité d'amorce : sélectionnez **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).
   - Connectivité d'instance : sélectionnez **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
   - Afficher les rubriques : sélectionnez la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.

   Remarque :
   Vous pouvez accéder Hermes à Diagnostics à l'avenir pour résoudre les problèmes de connectivité potentiels en revenant à cette étape de la configuration guidée ou en accédant à **Tous** > *`Service de messagerie Hermes`* > **Diagnostics**.

2. Générez des certificats pour une connexion sécurisée et Service de messagerie Hermes extrayez les événements de journal à partir de celle-ci.

   Vous allez utiliser ces certificats lors de la connexion de votre système externe.

   Configurez une connexion sécurisée à Service de messagerie Hermes. Pour plus d'informations, consultez Configurer une connexion sécurisée au service de messagerie Hermes pour LES . Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermes.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le créateur de journaux : choisissez les sources de journaux à exporter et configurez leurs filtres. Effectuez les tâches suivantes pour configurer le créateur de journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurer les sources de journal à exporter : créez un enregistrement source pour chacune des sources de journal que vous souhaitez exporter.

  Remarque :
  Les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape

  a. Sélectionnez **Nouveau** dans le coin supérieur droit

  b. Sélectionner un type de source

  c. Sélectionner une table

  d. Sélectionner un niveau de journal qui peut être utilisé pour contrôler la sortie de journalisation

  e. Sélectionnez ou créez une rubrique vers laquelle cette source de journal sera exportée. Si vous créez une nouvelle rubrique, renseignez les champs suivants :

  - **Nom** : nom de la rubrique que vous créez
  - **ID d'application** : Entrer `sn_logstoanalytics`
  - **Espace de noms** : entrer l'espace de noms par défaut
  - **Partition** : le champ partition d'une rubrique dans Hermes fait référence aux partitions dans lesquelles les données de la rubrique sont divisées. Il joue un rôle clé dans l'évolutivité et le parallélisme.

  f. Sélectionnez une condition **de type de filtre** pour transférer les journaux de manière sélective.

  Remarque :
  Les filtres sont différents selon le type de source sélectionné

  g. Sélectionner Mettre à jour
  Lorsqu'il est créé avec succès, il affiche le nom de la rubrique Hermes vers laquelle cette source de journal sera exportée. Notez le nom de la rubrique, vous en aurez besoin ultérieurement lors de la configuration de votre système de consommateur de journaux.

  Le champ Actif contrôle si cette source de journal va être exportée ou non. Si des erreurs s'affichent, revenez à la tâche Vérifier les diagnostics Hermes et vérifiez l'état d'Hermes.

- Valider le créateur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez voir les enregistrements de journaux actifs dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

  a. Sélectionner des rubriques externes

  b. Sélectionner les rubriques de la liste

  c. Sélectionnez une ligne avec votre rubrique de l'étape précédente (répertoriée dans Sources)

  d. Ajuster la date de début du message si nécessaire

  e. Sélectionnez **Afficher** pour afficher un message du journal qui a été exporté vers la rubrique

4. Connecter le consommateur Kafka : suivez ces tâches pour connecter le consommateur Kafka de votre choix afin d'extraire les événements de journal du Hermes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Identifier le consommateur Kafka : vous disposez de deux options en fonction de votre architecture d'analyse de journaux.
  - Si vous disposez de votre propre système Kafka et que vous le choisissez pour l'agrégation des journaux, vous pouvez vous connecter directement au service de messagerie Hermes via le protocole Kafka natif.
  - Si vous choisissez de connecter votre outil d'analyse de journaux directement au service de messagerie Hermes, vous devez déployer un connecteur Kafka pris en charge par votre système d'analyse de journaux (c'est-à-dire Splunk Connect pour Kafka).

  Remarque :
  Dans les deux cas, vous devrez travailler avec l'administrateur de ces systèmes pour coordonner la connexion avec le service de messagerie Hermes.

- Importer des certificats Hermes dans le système de consommateur Kafka : connectez-vous à votre système de consommateur Kafka et assurez-vous d'avoir les droits d'administrateur appropriés pour le configurer et le connecter à un système externe. Importez les certificats générés dans la tâche « Configurer une connexion sécurisée à la messagerie Hermes Messaging Service » dans votre connecteur Kafka ou votre serveur Kafka. Suivez les instructions de la documentation pour le consommateur Kafka que vous avez choisi.
- Configurer les processus Kafka : le service de messagerie Hermes est conçu pour la haute disponibilité. Deux processus sont nécessaires pour consommer les messages d'Hermes. Deux processus sont nécessaires car Hermes utilise une paire de clusters Kafka à des fins de basculement. Si un cluster tombe en panne, les données sont produites dans l'autre cluster Hermes Kafka.

  Dans votre système de consommateur Kafka, vous devrez créer deux processus de consommateur distincts pour vous connecter aux deux clusters Kafka Hermes. Pour les deux processus, vous spécifierez la même rubrique Hermes Kafka, mais vous devrez configurer deux adresses d'amorce distinctes :

  - <instance_name>.service-now.com:4100,<instance_name>.service-now.com:4101,<instance_name>.service-now.com:4102,<instance_name>.service-now.com:4103
  - <instance_name>.service-now.com:4200,<instance_name>.service-now.com:4201,<instance_name>.service-now.com:4202,<instance_name>.service-now.com:4203

  Remarques importantes :

  - Lorsque vous accédez à la rubrique Kafka à partir de systèmes externes, vous devez ajouter « snc.<nom d'instance>. » à la rubrique vers laquelle les journaux sont transférés.
  - Configurez chaque consommateur avec le même ID de groupe de consommateurs Kafka.
  - Installez votre magasin de clés et vos fichiers du magasin de clés de confiance dans un emplacement où vos consommateurs peuvent y accéder.
  - Si vos consommateurs le requièrent, spécifiez les propriétés des convertisseurs JSON Kafka pour désactiver les schémas : « key.converter.schemas.enable=false », « value.converter.schemas.enable=false »
- Vérifier que le consommateur Kafka extrait les journaux d'Hermes : vérifiez dans le consommateur Kakfa que vous avez choisi que vous pouvez extraire les événements de journal du service de messagerie Hermes.

Traduction automatique

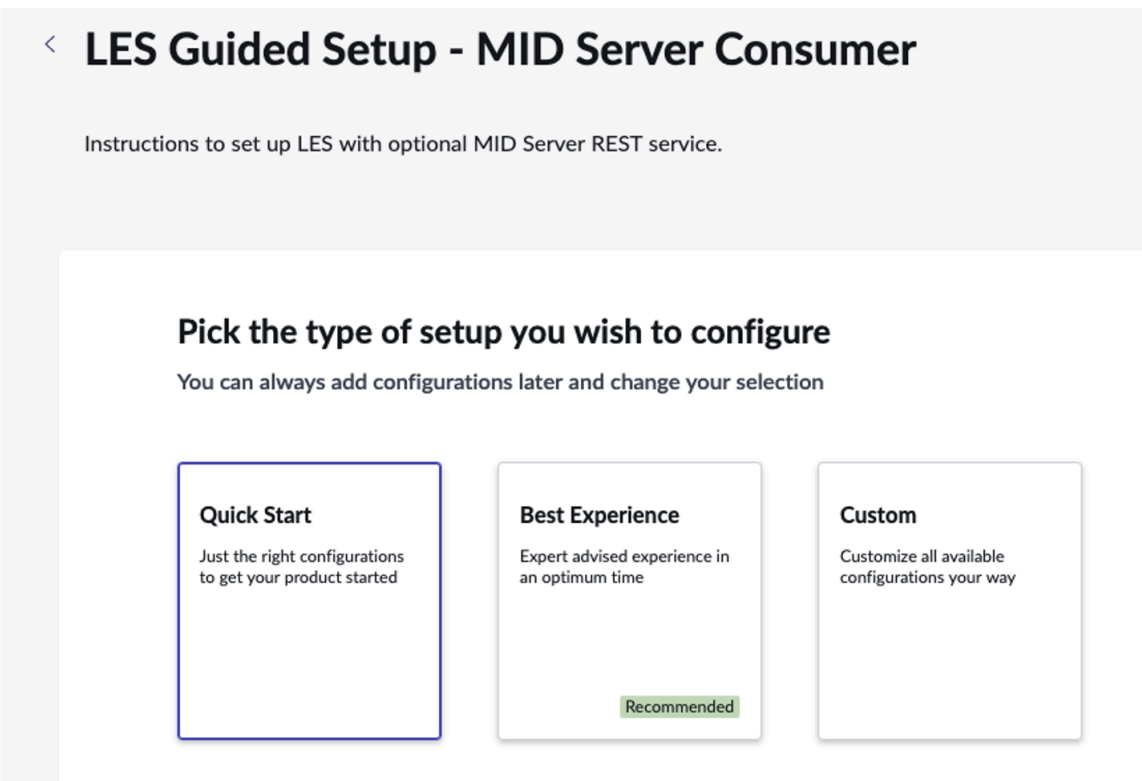
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consommateur de Serveur MID

Utilisez la configuration guidée pour exécuter pas à pas la configuration initiale de LES pour le consommateur de Serveur MID.

Page d'accueil de la configuration guidée

La page d'accueil de la configuration guidée contient une vue d'ensemble des types de configuration pour votre configuration guidée. Vous pouvez sélectionner votre type de configuration guidée, puis **sélectionner Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.



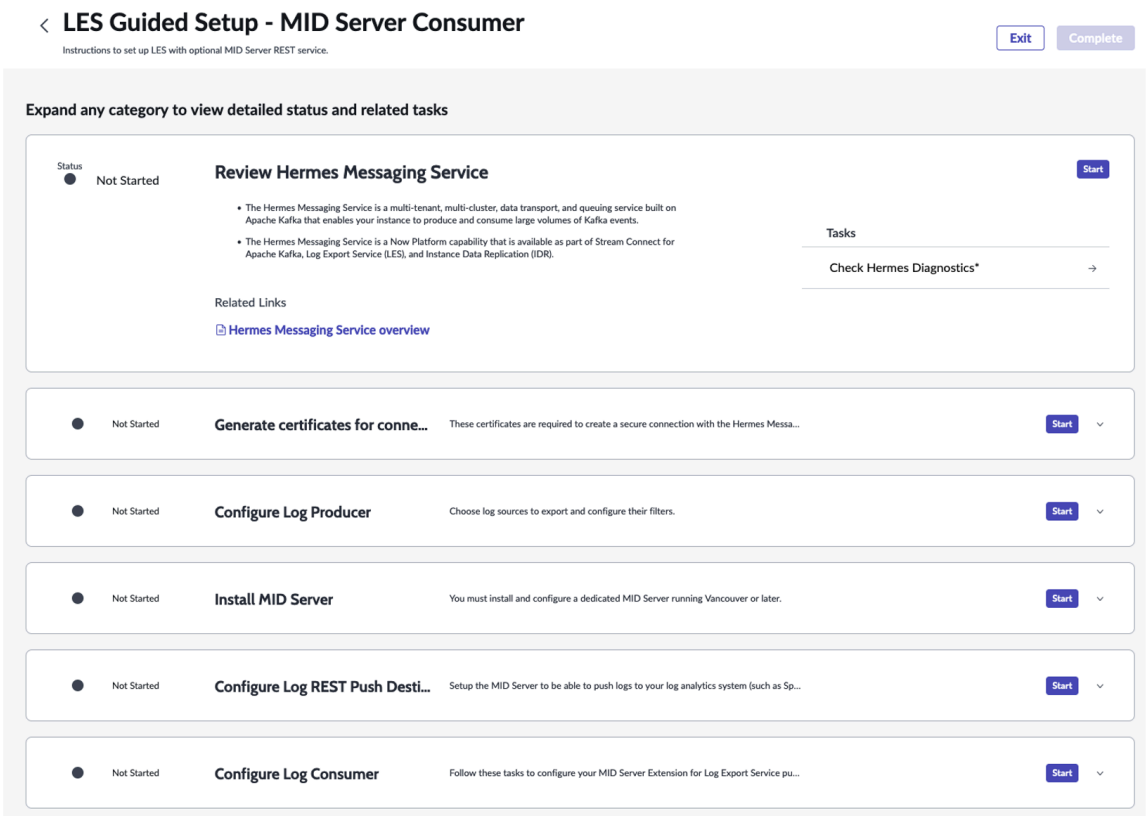
Les trois configurations de cette page, Démarrage rapide/Meilleure expérience/Personnalisé, fournissent les mêmes tâches et fonctionnalités. Un serveur MID dédié est nécessaire pour diffuser en continu les journaux de votre instance vers votre système d'analyse de journaux. Le serveur MID a besoin d'une configuration unique pour établir une connexion sécurisée au service de messagerie Hermes. Même si vous avez marqué une tâche comme terminée, vous pouvez revenir en arrière et la décocher à nouveau comme en cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la case **Modifier** pour la tâche que vous souhaitez décocher. La case **Marquer comme terminé** ne sera plus cochée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et des descriptions des catégories et des tâches associées. Vous pouvez cliquer sur la flèche de la liste déroulante pour afficher des informations sur la catégorie ou cliquer sur **Démarrer** pour ouvrir les étapes de la configuration guidée et commencer la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Effectuez les tâches de chaque catégorie en suivant les instructions de configuration.

Configuration guidée pour les consommateurs de Serveur MID

Implémentez les étapes suivantes pour une configuration guidée complète pour les consommateurs de Serveur MID.

Avant de commencer

Accédez à la **Service d'exportation de journaux (LES)** > **Consommateur de Serveur MID** > **Configuration guidée**. Sélectionnez le type de configuration que vous souhaitez configurer, puis sélectionnez **Continuer**.

Remarque :
Lors de l'installation de l'application Service d'exportation de journal , ServiceNow met en service l'infrastructure sous-jacente Service de messagerie Hermes . Sachez que ce processus peut prendre jusqu'à quelques heures à partir du moment où vous demandez l'installation de l'application Service d'exportation de journal .

Rôle requis : admin

Procédure

1. Passez en revue Service de messagerie Hermes les diagnostics.

   Nous vous recommandons de vérifier que l'outil Service de messagerie Hermes de diagnostic est en cours d'exécution, qui s'affiche à l'écran Hermes pendant cette étape. Si vous voyez une erreur « Page introuvable » sur cette page, Hermes elle n'est pas installée et vous devez contacter votre administrateur système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Informations sur la configuration : Les informations d'amorce suivantes sont utilisées pour se connecter au service de messagerie Hermes. Le « Starter Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et « Consumer Bootstrap 1 & 2 » sont utilisés pour récupérer des messages à partir de Hermes.
  - Amorce du créateur
  - Amorce de consommateur 1
  - Amorce de consommateur 2
- PKI d'instance : le composant d'infrastructure de clé publique d'instance (PKI) permet à une instance ServiceNow d'agir en tant qu'émetteur dans une hiérarchie de confiance X.509.
- Connectivité d'amorce : sélectionnez **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).
- Connectivité d'instance : sélectionnez **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
- Afficher les rubriques : sélectionnez la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.

Remarque :
Vous pouvez accéder Hermes à Diagnostics à l'avenir pour résoudre les problèmes de connectivité potentiels en revenant à cette étape de la configuration guidée ou en accédant à **Tous** > *`Service de messagerie Hermes`* > **Diagnostics**.

2. Générez des certificats pour une connexion sécurisée à Service de messagerie Hermes et extrayez les événements du journal à partir de celui-ci.

   Configurez une connexion sécurisée au service de messagerie Hermes. Pour plus d'informations, consultez Configurer une connexion sécurisée au service de messagerie Hermes pour LES . Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermes.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le créateur de journaux : choisissez les sources de journaux à exporter et configurez leurs filtres. Effectuez les tâches suivantes pour configurer le créateur de journaux.
   - Configurer les sources de journal à exporter : créez un enregistrement source pour chacune des sources de journal que vous souhaitez exporter.

     Remarque :
     Les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape

     Pour créer une source, accédez à **Service d'exportation de journaux** > **Sources**

     a. Sélectionnez **Nouveau** dans le coin supérieur droit

     b. Sélectionner un type de source

     c. Sélectionner une table

     d. Sélectionner un niveau de journal qui peut être utilisé pour contrôler la sortie de journalisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Sélectionnez ou créez une rubrique vers laquelle cette source de journal sera exportée. Si vous créez une nouvelle rubrique, renseignez les champs suivants :

- **Nom** : nom de la rubrique que vous créez
- **ID d'application** : Entrer `sn_logstoanalytics`
- **Espace de noms** : entrer l'espace de noms par défaut
- **Partition** : le champ partition d'une rubrique dans Hermes fait référence aux partitions dans lesquelles les données de la rubrique sont divisées. Il joue un rôle clé dans l'évolutivité et le parallélisme.

f. Sélectionnez une condition **de type de filtre** pour transférer les journaux de manière sélective.

> **Remarque :**
> Les options de type de filtre diffèrent selon le type de source sélectionné.

g. Sélectionner Mettre à jour
Lorsqu'il est créé avec succès, il affiche le nom de la rubrique Hermes vers laquelle cette source de journal sera exportée. Notez le nom de la rubrique, vous en aurez besoin ultérieurement lors de la configuration de votre système de consommateur de journaux.

Le champ Actif contrôle si cette source de journal va être exportée ou non. Si des erreurs s'affichent, revenez à la tâche Vérifier les diagnostics Hermes et vérifiez l'état d'Hermes.

- Valider le créateur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez voir les enregistrements de journaux actifs dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

  a. Sélectionner des rubriques externes

  b. Sélectionner les rubriques de la liste

  c. Sélectionnez une ligne avec votre rubrique de l'étape précédente (répertoriée dans Sources)

  d. Ajuster la date de début du message si nécessaire

  e. Sélectionnez **Afficher** pour afficher un message du journal qui a été exporté vers la rubrique

4. Installer Serveur MID : vous devez installer et configurer un serveur MID dédié exécutant Vancouver ou une version ultérieure.
Effectuez les tâches suivantes pour installer le serveur MID.

- Installez un serveur MID dédié : le serveur MID utilisé par le service d'exportation de journaux doit être dédié à cette fin uniquement et ne doit pas exécuter d'autres processus. Ceci est important pour garantir la livraison en temps opportun des messages du journal exportés à votre point de terminaison REST. Vous pouvez installer le nouveau serveur MID à l'aide de ou Use MID Server guided setup en l'installant manuellement. Pour l'installation manuelle, suivez d'abord la Configure MID Server network connectivity documentation puis la Installing the MID Server documentation ensuite.
- Valider le serveur MID : vous devez valider manuellement le serveur MID après son installation pour lui permettre d'exécuter des tâches d'automatisation. Pour valider le serveur MID que vous dédiez au LES, voir Validate the MID Server

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Configurer la destination push REST du journal : configurez le serveur MID pour pouvoir transmettre les journaux à votre système d'analyse de journaux (tel que Splunk).
   Procédez comme suit pour configurer la destination push REST du journal.

   - Ajouter des propriétés MID : vous devez ajouter des propriétés de serveur MID afin qu'il puisse se connecter à Hermes. Accédez à **Serveur MID** >**Propriétés** et définissez les valeurs appropriées pour chacune des propriétés énumérées ci-dessous.

Nom	Valeur
mid.les.kafka.ssl.truststore.password	<mot de passe>
mid.les.kafka.ssl.keystore.password	<mot de passe>
mid.les.kafka.ssl.key.mot de passe	<mot de passe>
mid.les.kafka.ssl.truststore.emplacement	<your_path>/<magasin de confiance>.p12
mid.les.kafka.ssl.keystore.emplacement	<your_path>/<magasin de clés>.p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc.<instance_name>.groupe1
mid.les.kafka.bootstrap.servers	<instance_name>.servicenow.com:4100,<instance_name>.servicenow.
mid.les.kafka.set2.bootstrap.servers	<instance_name>.servicenow.com:4200,<instance_name>.servicenow.

     Suivez ces notes pour obtenir certaines des valeurs ci-dessus

     - < mot de passe > est le mot de passe que vous définissez pour le magasin de clés et le magasin de clés de confiance
     - <your_path> s'agit du chemin d'accès au répertoire dans lequel vous conservez les fichiers du magasin de clés et du magasin de clés de confiance que vous avez téléchargés. Les certificats doivent se trouver sur le serveur sur lequel vous exécutez MID
     - <instance_name> est le nom de votre instance ServiceNow. Si vous n'êtes pas sûr, vous pouvez le trouver dans la table sys_properties
     - Vous pouvez obtenir les valeurs pour mid.les.kafka.bootstrap.servers et mid.les.kafka.set2.bootstrap.servers à partir de la page Diagnostics Hermes. Accédez à la **Service de messagerie Hermes** > **Diagnostics** et copiez les chaînes sous Consumer Bootstrap 1 et Consumer Bootstrap 2 respectivement.

   - Configurer la destination : créez un nouvel enregistrement de configuration de destination, qui définit le point de terminaison REST vers lequel cette extension transférera les journaux.

     Remarque :
     Les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape.

     a. Accédez à la **Service d'exportation de journaux (LES)** > **Destination Configurations**

     b. Créer un enregistrement de configuration

     c. Spécifiez l'URL de votre point de terminaison souhaité pour les sources de journal exportées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Recherchez ou créez des informations d'identification pour vous connecter à votre point de terminaison. Lors de la création des informations d'identification pour votre point de terminaison, notez que seuls les types d'informations d'identification suivants sont valides avec LES : Authentification de base, OAuth, clé API

e. Recherchez ou créez un script de transformation. Nous sommes fournis avec le script pré-écrit, **SplunkTransform** for Splunk

6. Configurer le consommateur de journaux : suivez ces tâches pour configurer l'extension de votre serveur MID à des fins de service d'exportation de journaux.

- Configurer le contexte du consommateur LES : Au cours de cette étape, vous allez mettre à jour l'enregistrement de consommateur LES pour qu'il s'exécute sur le serveur MID dédié que vous venez d'installer pour le service d'exportation de journaux. Accédez à la **Serveur MID** > **Extensions** > **Contexte du consommateur LES** et mettez à jour l'enregistrement du consommateur LES en définissant les champs suivants :
  - Sélectionnez « Consommateur LES » pour ouvrir l'enregistrement de contexte du Serveur MID.
  - Sélectionner un Serveur MID spécifique pour le champ « Exécuter sur »
  - Entrez le nom du MID que vous avez validé à l'étape précédente pour le champ « Serveur MID »

  Sélectionnez **Mettre à jour** pour enregistrer.

  Remarque :
  Nous livrons avec un contexte préconstruit. N'en créez pas un deuxième. Cela peut avoir des conséquences imprévues.

- Configurer le consommateur : crée un enregistrement Consommateur, qui représente le processus faisant partie de l'extension Serveur MID du service d'exportation de journaux. Accédez à la **Service d'exportation de journaux (LES)** > **Consommateurs** et créez un nouvel enregistrement de configuration spécifiant la rubrique Hermes à partir de laquelle récupérer les messages du journal et la destination vers laquelle les relayer. Lorsque vous sélectionnez le module **Consommateurs** , il affiche des informations sur le nom du consommateur et la configuration de destination.

  a. Créer un enregistrement de consommateur

  b. Choisir une rubrique source dans la liste déroulante

  c. Choisir la configuration de destination

  d. Démarrer le consommateur

- Vérifiez l'intégration du serveur MID : accédez à **Service d'exportation de journaux (LES)** > **État du consommateur** et affichez les champs État et Détails d'état de l'enregistrement défini. Les informations contenues dans ces champs signalent l'état actuel du processus en cours d'exécution sur le Serveur MID, y compris les erreurs qui ont pu se produire lors du relais de messages au point de terminaison REST. Il s'agit d'une page d'affichage d'état uniquement. Accédez à la **Service d'exportation de journaux (LES)** > **Consommateurs** Si vous souhaitez créer un nouvel enregistrement de consommateur. #Si l'état Consommateur indique que le processus a démarré, vous devriez être en mesure d'inspecter votre point de terminaison pour afficher les journaux qui lui ont été relayés. En outre, vous pouvez afficher les journaux sur le serveur MID pour voir s'il existe des détails supplémentaires sur les erreurs qui peuvent être

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

rencontrées. Vous pouvez également activer la journalisation de débogage sur Serveur MID pour obtenir des informations supplémentaires si nécessaire.

Remarque :
Si vous apportez une modification à l'un des enregistrements de consommateur, elle s'affiche sur la page d'affichage État du consommateur. Si vous sélectionnez un nom d'enregistrement de consommateur dans la liste État du consommateur, le formulaire de consommateur de l'enregistrement sélectionné s'ouvre. Vous pouvez ensuite mettre à jour le nom et la configuration de destination de l'enregistrement sélectionné.

Prise en charge multi-consommateurs à l'aide de MID Servers uniques

Vous pouvez désormais gérer avec précision la consommation de journaux avec un nouveau système multi-consommateurs, permettant des consommateurs et des serveurs MID dédiés pour chaque flux de journal spécifique.

Le système prend désormais en charge la consommation de journaux multi-consommateurs, ce qui signifie que chaque source de journal peut être consommée séparément avec sa propre rubrique dédiée.

Auparavant, tous les journaux étaient utilisés à partir de la même rubrique. Cependant, avec le nouveau concept multi-sujets, vous pouvez créer plusieurs consommateurs pour différents sujets. Pour créer un consommateur, vous pouvez sélectionner les éléments suivants :

- Une rubrique spécifique dans le menu déroulant
- Configuration de la destination respective
- Contexte de consommateur respectif

Remarque :
À partir de la version Zurich, le **contexte Consommateur** est un nouveau champ ajouté au formulaire Consommateur. Chaque contexte de consommateur est associé à un serveur MID unique.

Pour créer plusieurs consommateurs, vous devez sélectionner des rubriques distinctes pour chaque consommateur, ce qui nécessite à son tour de créer des enregistrements de contexte de consommateur distincts et ses serveurs MID uniques correspondants.

Traitement parallèle avec plusieurs serveurs MID

L'un des principaux avantages de cette architecture multi-consommateurs est la possibilité d'exécuter plusieurs consommateurs en parallèle. Ce traitement parallèle améliore considérablement le débit global et l'efficacité de la consommation de grumes, ce qui permet au système de traiter de plus grands volumes de données de grumes diverses plus efficacement qu'auparavant.

Configurer une connexion sécurisée au service de messagerie Hermes pour les LES

Sécurisez vos rubriques Kafka en générant un certificat signé par l'instance ServiceNow® .

Avant de commencer

La configuration nécessite une Service de messagerie Hermes coordination avec votre administrateur réseau et votre administrateur Kafka. Collaborez avec votre administrateur réseau pour obtenir les certificats de sécurité requis et ouvrir les ports requis. Travaillez avec votre administrateur Kafka pour vous assurer que votre environnement Kafka est correctement configuré et que vos applications peuvent s'y connecter à l'aide Service de messagerie Hermes du protocole Kafka standard.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que la configuration suivante est en place :

- Le Service de messagerie Hermes est activé. Consultez Activating the Hermes Messaging Service .
- Le module d'extension Key Management Framework (com.glide.kmf.global) est activé.
- La table Certificats [sys_kmf_certificate] contient un certificat d'autorité ServiceNow de certification racine de l'instance.
- L'instance n'est pas configurée avec une URL personnalisée. Les URL personnalisées ne sont pas prises en charge avec le générateur de certificats PKI d'instance.

Rôle requis : hermes_admin, sn_kmf.cryptographic_manager ou admin

Pour en savoir plus sur l'affectation des rôles KMF, reportez-vous à la section Rôles installés avec Key Management Framework.

Procédure

1. Accédez à la **Tous** > **Générateur de certificats** > **Générateur de certificats PKI de l'instance**.
2. **Facultatif :** Contrôlez l'accès aux rubriques en configurant les listes de contrôle d'accès (ACL) au niveau de l'espace de noms ou de la rubrique.
   Le titulaire du certificat bénéficie d'un accès en lecture ou en lecture/écriture aux rubriques de l'espace de noms ou de la rubrique existante que vous avez sélectionnée.
3. Configurez la sécurité pour le Service de messagerie Hermes.
   a. Revenez à la page Générateur de certificats PKI de l'instance.
   b. Saisissez un mot de passe de magasin de clé dans le champ **Mot de passe du certificat** .
   c. Sélectionnez **Générer**.
   Le système génère un certificat signé par l'instance dans la table Certificats [sys_kmf_certificate], crée un magasin de clés et crée un magasin de confiance.

   Si l'accès restreint pour l'appelant n'est pas autorisé pour le générateur de certificats IPKI, une erreur d'accès entre périmètres s'affiche. Contactez Service client et assistance pour obtenir de l'aide afin d'autoriser l'accès restreint pour l'appelant. Pour résoudre ce problème, Service client et assistance peut faire référence à source_scope=76f9d51369115083f4ea77aab1677cc0 dans la table Privilèges d'accès restreint pour l'appelant [sys_restricted_caller_access].
4. Enregistrez une copie du magasin de clés en sélectionnant **Télécharger le magasin de clés**.
5. Enregistrez une copie du magasin de clés de confiance en sélectionnant **Télécharger le magasin de clés de confiance**.
6. Copiez les fichiers du magasin de clés et du magasin de clés de confiance sur chaque client producteur et consommateur qui se connectera au Service de messagerie Hermes.

Résultats

Vous pouvez maintenant créer une connexion sécurisée au Service de messagerie Hermes.

Remarque :
Vous devez utiliser le magasin de clés que vous avez généré à l'aide du générateur de certificats PKI d'instance pour vous connecter à Hermes. Les magasins de clés générés personnalisés qui ne sont pas créés conformément à la ServiceNow documentation ne sont pas pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

.

Utilisation (Service d'exportation de journal LES)

Utilisez le LES pour examiner le tableau de bord du rapport de journal.

Examiner le rapport du journal

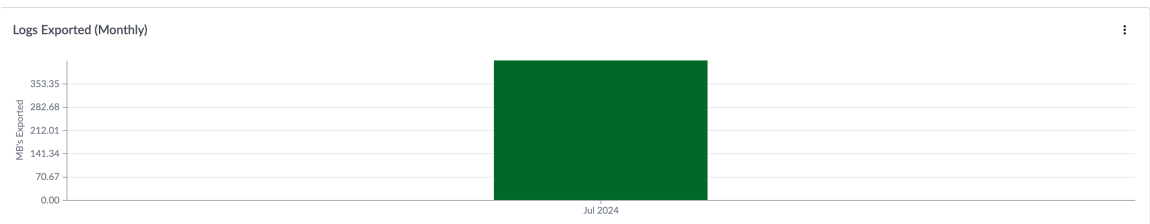
Analysez la taille de chaque journal de données en examinant le tableau de bord du rapport de journal.

Avant de commencer

Rôle requis : admin ou sn_logstoanalytics.admin

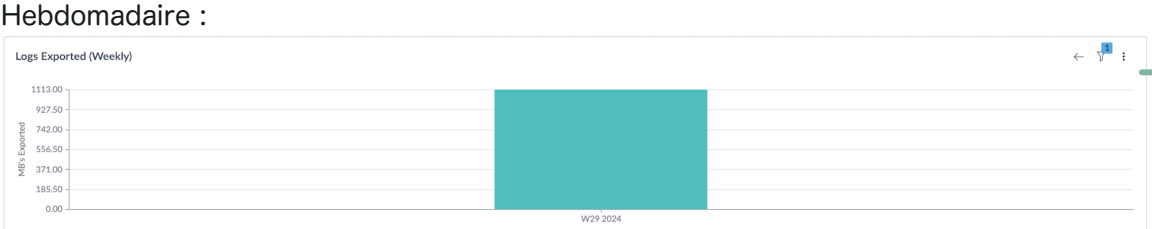
Procédure

1. Accédez à la **Tous** > **Service d'exportation de journaux** > **Rapports**.
2. Examinez les données du journal dans les widgets suivants.
   - Journaux exportés (mensuel) : affiche les mégaoctets exportés par mois dans la vue initiale. Vous pouvez analyser le graphique pour afficher les données de chaque semaine ou données quotidiennes. Vous pouvez afficher les données des 395 derniers jours.

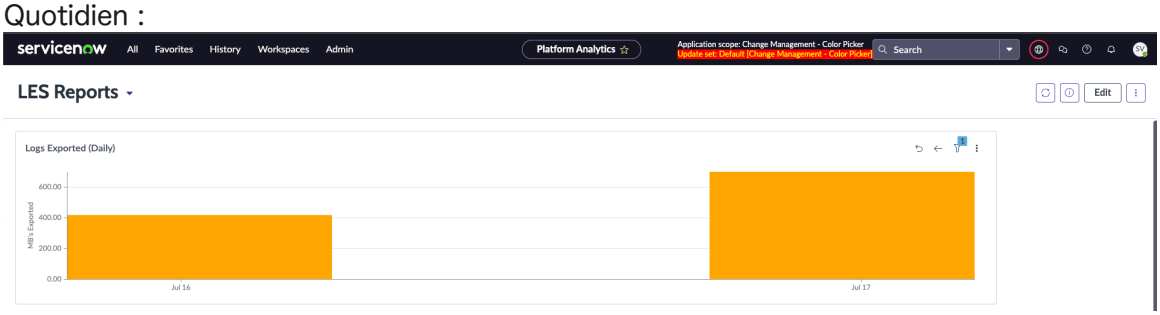


Remarque :
Cliquez sur les flèches dans le coin supérieur droit du widget pour explorer les données. Vous pouvez également revenir aux données parentes.

Hebdomadaire :



Quotidien :

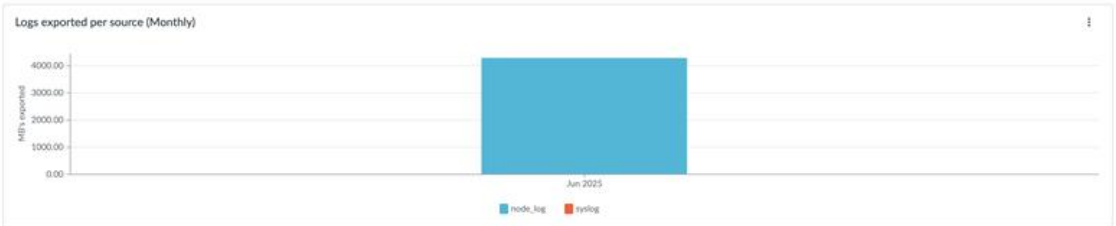


Les données de ce rapport reflètent la collecte effectuée 4 heures auparavant.

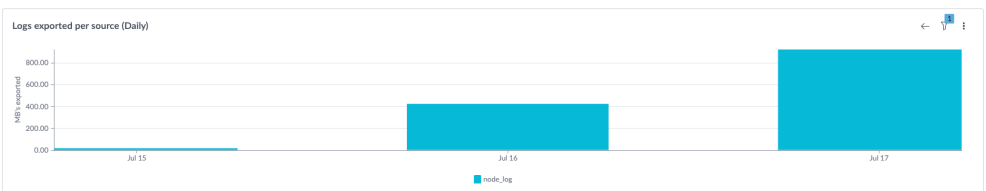
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

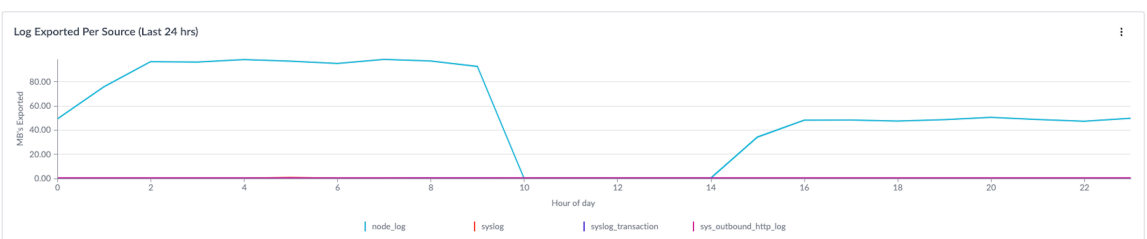
- Journaux exportés par source (mensuel) : ce widget affiche le type de journaux exportés sur une base mensuelle. Vous pouvez également analyser pour voir les données de journal hebdomadaires et quotidiennes. Vous pouvez afficher les données des 395 derniers jours.



Remarque :
Vous pouvez sélectionner ou désélectionner la source à partir de laquelle vous souhaitez afficher les données. Les sources à partir desquelles vous pouvez afficher les journaux sont : node_log, syslog, syslog_transaction et sys_outbound_http_log.



- Journal exporté par source (dernières 24 heures) : il affiche les données des dernières 24 heures. Le graphique progresse chronologiquement de gauche à droite sur une échelle de 24 heures, les données les plus anciennes (24e heure) étant positionnées à droite et les dernières données sur le côté gauche du rapport. Vous pouvez sélectionner ou désélectionner la source à partir de laquelle vous souhaitez afficher les données. Les sources à partir desquelles vous pouvez afficher les journaux sont : node_log, syslog, syslog_transaction et sys_outbound_http_log.

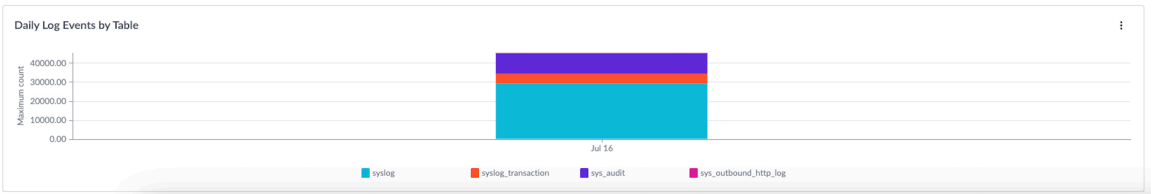


Remarque :
En fonction de l'heure de la journée à laquelle vous vérifiez ces données, le widget se met à jour dynamiquement pour refléter exactement les dernières 24 heures.

- Événements de journal quotidiens par table : affiche les événements de journal générés par chaque table de journal par jour. Vous pouvez sélectionner ou désélectionner les tables à partir desquelles vous souhaitez afficher les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Les tables à partir desquelles vous pouvez afficher les événements de journal sont : syslog, syslog_transaction, sys_audit et sys_outbound_http_log.

Service d'exportation de journal Références (LES)

Retrouvez toutes les informations diverses sur les ERP dans la section référence.

Service d'exportation de journal rôles

Service d'exportation de journal est installé avec ces rôles.

Administrateur d'application [sn_logstoanalytics.admin]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

Ce rôle est installé en même temps que l'application LES et permet à un non-administrateur d'utiliser l'application.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Élevé

Indique s'il s'agit d'un rôle élevé. Les rôles élevés ne sont pas affectés à des utilisateurs ou à des groupes, et doivent être utilisés par Elevation. Pour plus de détails, voirAccéder à un rôle privilégié.

N°

Considérations spéciales

Aucun.

Administrateur système [administrateur]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

Le rôle administrateur est requis pour la configuration de l'application du magasin LES.

Contient des rôles

Liste des rôles contenus dans le rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_templated_snip.template_snippet_admin
- [sn_employee.admin]
- taxonomy_admin
- sn_ace.ace_user
- [sn_hr_sp.esc_admin]

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Élevé

Indique s'il s'agit d'un rôle élevé. Les rôles élevés ne sont pas affectés à des utilisateurs ou à des groupes, et doivent être utilisés par Elevation. Pour plus de détails, voir Accéder à un rôle privilégié.

N°

Considérations spéciales

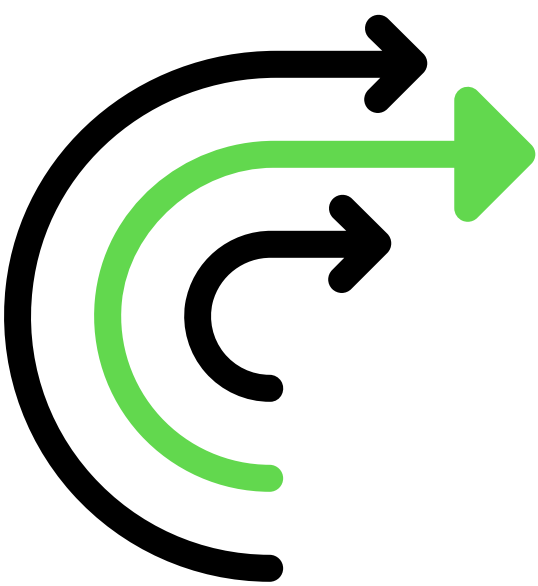
Aucun.

Journaux

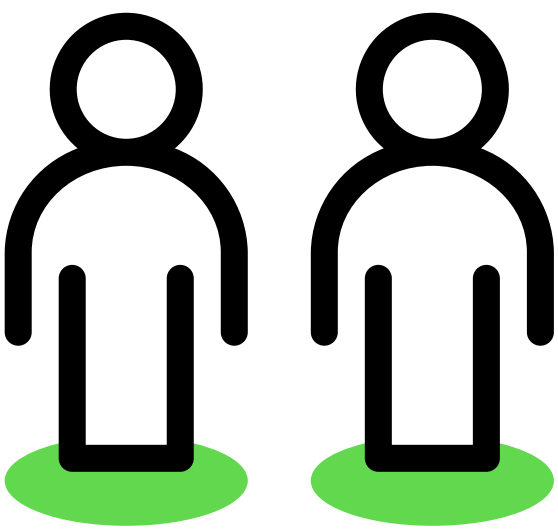
Le module Journaux fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Premiers pas

Journaux système



Journalisation, audit et erreurs



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et agir en temps opportun.

Journaux système

Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Accédez aux journaux suivants à partir du module Journaux système :

Journal	Description
Transactions	Toute l'activité de l'application pour une instance.
E-mail et push	Toutes les notifications par e-mail et tous les messages push envoyés depuis toutes les instances du système.
Journaux des événements	Tous les événements système qui se produisent au sein du système.
Importer	Activité d'importation de données au sein de la plateforme.
Changements de tables	Changements apportés à toutes les tables du système.
Connexion des services Web sortants	Toutes les demandes de services Web sortantes telles que les demandes REST et SOAP.
Images de signatures	Signatures électroniques pour le pavé de signature RH.
Système	Avertissements et erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur le serveur.

Utilisez le navigateur de fichier journal pour rechercher et télécharger des journaux. Vous pouvez également rechercher des journaux archivés dans l'historique des journaux.

Autres journaux

Votre instance propose d'autres journaux en plus de ceux du module Journaux système. Par exemple, fournit l'historique des mises à niveau et les Module de diagnostic du système journaux de requêtes lentes, que vous pouvez utiliser pour avoir un aperçu de la façon dont les requêtes affectent les performances de la plateforme. Enregistre Table de mises à jour du client chaque modification apportée au système.

Journal système

Affichez les avertissements et les erreurs pour les processus, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur le serveur.

Les informations suivantes sont suivies dans le journal système :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Workflows
- Configuration
- Sessions de messagerie instantanée
- Transactions pour chaque vue de chaque page du système, y compris les temps de chargement pour le réseau, le serveur et le navigateur
- E-mail entrant et sortant
- Événements déclenchés dans le système
- Importations et intégrations
- Avertissements système, erreurs et journaux de script
- Informations de mise à niveau pour toute activation de module d'extension, ensemble de mises à jour ou mises à niveau système

Les entrées de journal s'affichent uniquement pour le jour en cours. Pour afficher d'autres fichiers journaux, utilisez le navigateur de fichier journal. Ce journal fournit les informations suivantes pour toutes les occurrences :

Journal système

Champ	Description
Créées	Date et heure de l'activité de journalisation pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Niveau	Type de message. Les niveaux sont Débogage, Erreur, Avertissement et Information. • Un avertissement est une erreur qui a été traitée et récupérée. • Une erreur est quelque chose qui doit être corrigé.
Message	Message généré par le système concernant la nature de l'événement.
Source	Nom du processus ou de la zone affectée par l'événement. Par exemple, la source de l'occurrence peut être EMAIL ou Memory.
Source Package	Nom du package applicatif associé à l'occurrence. Cliquez sur le nom pour afficher l'enregistrement de l'application du magasin [sys_store_app] pour ce package.

Journalisation du workflow

- Chaque activité exécutée, y compris :
  - Date et heure de début
  - Date et heure de fin
  - État, par exemple, Terminé, Annulé, Expiré, Erreur
  - Résultat
  - Description de panne, en cas d'erreur
- Historique de la transition, y compris :
  - Heure de la transition
  - Activité transférée de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - Activité transférée vers
  - Quelle transition a été déclenchée
- Journal de workflow, y compris toutes les instructions de journal ajoutées au workflow

Informations sur la configuration

- Action effectuée, y compris l'insertion, la mise à jour et la suppression
- Catégorie de changement
- Commentaires enregistrés avec le changement
- Nom du changement
- Différence XML du changement
- Ensemble de mises à jour auquel le changement est associé
- Date et heure du changement
- Utilisateur ayant effectué le changement
- Table où le changement a été apporté
- Nom de l'objet en cours de modification
- Type d'objet en cours de modification
- Voir le changement effectué dans pour les changements apportés aux formulaires ou aux listes

Journaux de transactions

Le journal des transactions enregistre toute l'activité du navigateur pour une instance. Pour faciliter le débogage des problèmes système, vous pouvez filtrer les journaux des transactions par périmètre de l'application, en limitant les transactions qui s'affichent aux seules transactions provenant de périmètres spécifiques.

Accéder aux journaux des transactions en accédant à **Tous** > **Journaux système** > **Transactions**. Le journal des transactions fournit les informations suivantes pour toutes les activités.

Champ	Description
Créées	Date et heure de l'action de l'application pour les paramètres régionaux de l'ordinateur qui exécute l'instance.
Type	Type de transaction enregistrée.
Créé par	Utilisateur qui a créé cette activité.
Application d'origine	Périmètre de l'application d'où provient la transaction. Global s'affiche si la transaction provient du champ d'application global.
Temps de réponse	Délai de réponse aller-retour pour la demande d'application, en millisecondes.
Délai réseau	Temps de latence de la réponse du réseau après l'envoi de la demande d'application, en millisecondes.
Longueur de sortie	Taille de la chaîne de sortie envoyée par l'instance à l'application, en octets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Compte SQL	Nombre de commandes SQL Server exécutées pour cette activité.
Nombre de règles métier	Nombre de règles métier exécutées pour cette activité.
Heure de règle métier	Temps écoulé pour l'exécution des règles métier pour cette activité.
URL	Application ou module auquel l'application cliente est connectée.
ID système	Identificateur généré par le système de l'instance client effectuant la demande. Cet ID est utilisé pour les environnements de grappe dans lesquels plusieurs instances (nœuds) communiquent avec la base de données.
Adresse IP	Adresse IP du client effectuant la demande.
Compressé avec GZIP	Indication de la demande d'une page Web compressée par l'application.
Protocole	Protocole HTTP utilisé par l'application pour cette instance.

Minuteurs des transactions client

Le module d'extension Client Transaction Timings améliore les journaux système en fournissant des informations supplémentaires sur la durée des transactions entre le client et le serveur.

Vous pouvez rechercher les problèmes de performances jusqu'à leur source en affichant où le temps est consommé et comment le temps a été utilisé au cours d'une transaction.

Ce module d'extension nécessite l'activation de l'indicateur de délai de réponse Indicateur de délai de réponse et collecte des informations à partir des navigateurs suivants :

- Firefox
- Internet Explorer
- Chrome

Informations sur les transactions clientes

L'installation du module d'extension ajoute le module *Transactions clientes* à l'application *Journaux système* . Il fournit une liste de toutes les transactions enregistrées entre le client et le serveur au cours du dernier jour :

Informations sur les transactions clientes

Champ	Description
Créées	Moment où la transaction a été enregistrée.
Temps de réponse	Nombre de ms consacrées par le serveur à l'exécution de la transaction.
Temps de règle métier	Nombre de ms consacrées aux règles métier déclenchées par la transaction.
Temps SQL	Nombre de ms consacrées à la base de données SQL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations sur les transactions clientes (suite)

Champ	Description
Temps de réponse client	(Load_completion_time) - (start_time). Il inclut le temps du serveur.
Délai réseau du client	Nombre de ms passées par le réseau via lequel le client se connecte.
Temps de navigation	Nombre de ms passées par le navigateur au cours de la transaction.
Heure du script client	Nombre de ms passées à exécuter des scripts clients.
Heure de politique d'interface utilisateur	Nombre de ms passées à exécuter la politique d'interface utilisateur.
Type	Type de transaction : • Formulaire • Liste • Autre
Table	Nom de la table qui est apparue. Par exemple, incident, change_request.
Vue	Vue de ce formulaire/liste.

Informations détaillées sur le client

Une répartition plus détaillée des minutages du client pour tous les rendus de formulaires (mais pas pour le rendu de liste) est également suivie. Pour afficher les détails, explorez un enregistrement de transaction client particulier et observez la liste connexe en bas de l'écran.

Informations détaillées sur le client

Champ	Description
Ordre	Ordre pendant le chargement au cours duquel cette opération s'est produite.
Type	Type d'opération.
Nom	Nom descriptif de cette opération particulière
Durée	Nombre de ms nécessaires à cette opération.

Journaux push

Consultez le journal push pour suivre l'état des notifications push qui sont mises en file d'attente pour être envoyées à partir de votre système.

Pour afficher le journal push, accédez à **Journaux système** > **Notifications push**. Les utilisateurs doivent avoir le rôle d'administrateur ou de push_admin pour afficher le journal push.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Transmettre par push les champs de journal

Champ	Description
Réclamation	Numéro d'identification généré par la tâche planifiée qui envoie la notification push. Ce numéro est appliqué au champ **Réclamation** pour garantir la cohérence entre plusieurs travaux planifiés push.
Charge utile	Contenu de la notification push.
Nombre de files d'attente	Nombre de fois où le système a essayé d'envoyer la notification push. L'état de la notification push est lié à son nombre de files d'attente. • Si le nombre de files d'attente est de 0 pendant plus longtemps que prévu, aucune tâche planifiée n'essaie d'envoyer la notification push. • Si le nombre de files d'attente est supérieur à 0 et que le **type** est **réussi**, vous pouvez en déduire qu'il s'agit du nombre de fois où le système a essayé d'envoyer la notification push avant l'envoi final. • Si le nombre de files d'attente atteint 10, le système arrête d'essayer d'envoyer la notification push. Le **type** devient **échec**.
ID de demande	Numéro d'identification unique de la notification push. Tout comme l'ID de message d'un e-mail, l'ID de demande est utilisé comme jeton de corrélation pour la notification push.
Type	État indiquant si la notification push a été envoyée. La colonne Type peut avoir ces valeurs : • **ÉCHEC** : le message n'a pas pu être envoyé. • **pending** : le message est mis en file d'attente pour traitement. • **réussite** : le message a été envoyé avec succès, mais pas nécessairement reçu par l'appareil mobile.

Information associée

Travaux planifiés

Journal des e-mails système et boîtes aux lettres

Le journal d'e-mail système enregistre tous les e-mails créés ou reçus par l'instance. Les boîtes aux lettres système sont des vues filtrées de ce journal.

Chaque e-mail de notification créé ou reçu par l'instance est enregistré dans un enregistrement d'e-mail [sys_email]. Vous pouvez accéder à un journal de ces enregistrements à l'adresse **Journaux système** > **E-mails**.

Les boîtes aux lettres système sont des vues filtrées de la table des e-mails [sys_email]. L'instance affecte un enregistrement d'e-mail à une boîte aux lettres système en fonction des valeurs des champs **Type** et **État** . Pour plus d'informations, voir Boîtes aux lettres système .

Les champs suivants peuvent être inclus dans la mise en page du journal système et de n'importe quelle boîte de réception système :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal d'e-mail

Champ	Description
Boîte de réception	La boîte de réception système qui répertorie cet enregistrement d'e-mail. L'instance définit la valeur de ce champ en fonction des valeurs des champs **Type** et **État** .
État	État actuel de l'e-mail (Erreur, Ignoré, Traité ou Prêt).
Type reçu	Type d'e-mail entrant (Aucun, Transférer, Nouveau ou Répondre).
Type	Le statut de l'e-mail. Les choix possibles sont les suivants : • reçu : le serveur a reçu cet e-mail. • reçu – ignoré : le serveur a reçu cet e-mail, mais il a été ignoré par l'instance à des fins d'action sur e-mail entrant. En règle générale, ces e-mails sont soit des spams, soit des réponses automatiques. Consultez le champ Chaîne d'erreur pour plus d'informations. • envoyer : échec : le serveur a tenté d'envoyer l'e-mail et a échoué. Consultez le champ Chaîne d'erreur pour plus d'informations. • envoyer : ignoré : le serveur a ignoré l'envoi de cet e-mail. En règle générale, il s'agit d'un e-mail qui a été généré, mais qui n'a pas d'adresse e-mail du destinataire ou qui est un e-mail en double. Consultez le champ Chaîne d'erreur pour plus d'informations. • send - ready : l'e-mail est prêt à être envoyé, mais n'a pas été envoyé par le serveur de messagerie. En règle générale, un e-mail ne reste dans cet état que pendant une courte période. • envoyer - traduction - prêt : l'e-mail est généré pendant la traduction de l'e-mail et envoyé. En règle générale, un e-mail ne reste dans cet état que pendant une courte période. • sent : l'e-mail a été envoyé par l'instance sans erreur ni problème.
Cible	Référence de l'ID de document à l'enregistrement si l'e-mail est généré par une insertion, une mise à jour ou la suppression d'un enregistrement particulier.
Utilisateur	Nom de l'utilisateur, issu de l'enregistrement utilisateur, de l'instance à partir de laquelle la notification par e-mail a été envoyée. **Remarque :** Il s'agit d'un champ de chaîne.
Type de notification	Type de notification. Les choix possibles sont les suivants : • Aucun • SMS • SMTP
UID	ID unique de l'e-mail stocké sur le serveur.
Créées	Date et heure de l'activité d'e-mail pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Supprimé	Pour l'e-mail entrant, indique si l'e-mail a été supprimé du serveur de messagerie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal d'e-mail (suite)

Champ	Description
Pondération	Poids de l'e-mail, qui détermine la priorité d'envoi par rapport aux autres notifications de la même table.
Importance	Indication que l'e-mail a été envoyé avec un niveau d'importance modifié, tel que Urgent.
Événement et notification d'origine	Pour les e-mails générés par des notifications, liste incorporée qui stocke l'événement et la notification à l'origine de l'e-mail.
Objet	L'objet de l'e-mail. Pour les notifications, vous créez le texte de l'objet dans **Notification système** > **E-mail** > **Notifications**.
Message d'erreur	La chaîne d'erreur capturée à partir du serveur de messagerie pour déterminer pourquoi l'e-mail n'a pas été envoyé. Ceci est journalisé uniquement si l'envoi de l'e-mail a échoué.
Destinataires	Les adresses e-mail des destinataires.
Détails	Le corps de l'e-mail, affiché dans un balisage HTML brut. Utilisez le lien connexe Aperçu du corps HTML pour afficher le corps du texte comme HTML rendu.
Type de contenu	Le type de contenu d'e-mail.
En-têtes	Tous les en-têtes incorporés dans l'e-mail.

Journaux des événements

Le journal des événements enregistre tous les événements système qui se produisent dans le ServiceNow AI Platform.

Ce journal fournit les informations suivantes pour tous les événements qui se produisent :

Journal des événements

Champ	Description
Créées	Date et heure de l'événement pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Nom	Nom de l'événement tel que répertorié dans le registre des événements.
URI	Requête HTTP qui a généré l'événement.
Param1	Valeur spécifique à l'événement qui dépend de l'événement et du destinataire.
Parm2	Valeur spécifique à l'événement qui dépend de l'événement et du destinataire.
Table	Table de base de données utilisée pour cet événement.
Traité	Date et heure auxquelles le traitement de l'événement a commencé. Cette heure reflète les paramètres régionaux de la machine qui exécute l'instance.
Temps de traitement	Temps nécessaire pour traiter cet événement, en millisecondes.
File d'attente	Nom de la file d'attente du processeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux d'importation

Le journal d'importation affiche des informations au format détaillé sur toute activité d'importation de données au sein de la plateforme.

Pour une vue plus détaillée des jeux d'importation qui ont produit un journal particulier, consultez **Ensembles de données à importer** > **Historique de transformation**.

Ce journal fournit les informations suivantes pour toutes les importations :

Journal d'importation

Champ	Description
Créées	Date et heure de l'importation pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Niveau	Type de message affiché. Pour les fichiers d'importation, le niveau est Information.
Message	Message généré par le système concernant l'état de l'importation.
Source	Nom de la source externe de l'importation, telle qu'une intégration.

Module de diagnostic du système

L'application Diagnostics du système fournit des journaux relatifs à la plateforme.

Ces journaux sont disponibles :

Historique des mises à niveau

Suit chaque mise à niveau d'une instance.

Requêtes lentes

Fournit un aperçu de la façon dont les requêtes affectent les performances de la plateforme. Voir Utiliser un journal des requêtes lentes .

Table de mises à jour du client

Les changements apportés au système sont enregistrés chronologiquement dans la table des mises à jour du client [sys_update_xml]. Il y a quelques exceptions, comme indiqué ci-dessous.

Pour accéder à cette table, entrez sys_update_xml.list dans le filtre de navigation. Pour plus d'informations sur les ensembles de mises à jour, voir Ensembles de mises à jour système .

Les informations suivantes sont stockées pour chaque mise à jour :

Table de mises à jour du client

Champ	Description
Nom	Nom qui identifie l'enregistrement mis à jour.
Créées	Date et heure de création de l'enregistrement de mise à jour du client.
Créés par	L'utilisateur qui a effectué le changement.
Type	Type de la mise à jour.
Mis à jour	Date et heure de la mise à jour de l'enregistrement de mise à jour du client.
Mis à jour par	L'utilisateur qui a effectué la mise à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table de mises à jour du client (suite)

Champ	Description
Mises à jour	Nombre de fois que l'enregistrement a été mis à jour.
Nom cible	Nom de l'élément qui a été modifié.
Vue	Vue du formulaire qui a été modifiée s'il s'agissait d'un changement de mise en page de formulaire.
Charge utile	Contenu XML de l'enregistrement après le changement.
Ensemble de mises à jour distant	Référence à cet ensemble de mises à jour si le changement a été effectué par un ensemble de mises à jour distant.
Ensemble de mises à jour local	L'ensemble de mises à jour auquel le changement est associé.

Remarque :
Certains changements d'application ne sont pas représentés par les enregistrements de mise à jour du client (sys_update_xml) Exemples :

- Types de métadonnées où updateSynch = false
- Changements en cascade apportés aux tables et aux champs, tels que les changements de nom d'affichage
- Références de métadonnées non résolues provenant d'autres applications (n'entraînant aucune « valeur d'affichage » sur l'élément)
- sys_id changements pour la coalescence de fichiers
- Changements apportés au flux/aux actions de flux susceptibles de générer des sys_documentation
- ua_table_license_config enregistrements générés lors de la création de la table
- Tâches exécutées en arrière-plan, telles que le traitement du langage naturel
- Tickets où sys_update_xml est modifié ou supprimé manuellement

Pour en savoir plus, consultez Valider les modifications .

Historique du journal

Le système utilise la rotation de table et l'extension de table pour archiver les journaux plus anciens.

Par défaut, le système utilise le calendrier suivant pour archiver les journaux communs :

Calendrier d'archivage de journaux commun

Table	Archiver le calendrier	Rotations	Type
Événement [ecc_event]	Tous les jours	7	Rotation
File d'attente [ecc_queue]	Tous les jours	7	Rotation
Événement [sysevent]	Tous les jours	7	Rotation
Journal [syslog]	Chaque semaine	8	Rotation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier d'archivage de journaux commun (suite)

Table	Archiver le calendrier	Rotations	Type
Journal des transactions [syslog_transaction]	Chaque semaine	8	Rotation
E-mail [sys_email]	Tous les 30 jours	8	Extension

Utiliser le navigateur de fichier journal

L'instance fournit les utilitaires Navigateur de fichier journal et Téléchargement de fichier journal.

Utiliser **Journaux système** > **Utilités** > **Navigateur de fichier journal de nœud** pour afficher une entrée de journal système. Vous pouvez rechercher des fichiers journaux à l'aide des filtres suivants :

Navigateur de fichier journal

Champ	Description
Heure de début	Date et heure de début de la plage que vous souhaitez rechercher, pour les paramètres régionaux de l'ordinateur exécutant l'instance.
ID de session	Chaîne hexadécimale générée par le système qui identifie la session qui a généré l'entrée de journal.
Heure de fin	Date et heure de fin de la plage que vous souhaitez rechercher, pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Message	Description de l'occurrence générée par le système.
Niveau	Type de message affiché. Les niveaux sont Débogage, Erreur, Avertissement et Information. Un avertissement est une erreur qui a été traitée et récupérée. Une erreur est quelque chose qui doit être corrigé.
Nom de thread	Identificateur généré par le système du thread qui a créé le fichier journal.
Lignes max.	Nombre maximal d'enregistrements renvoyés pour un filtre particulier.

L'instance crée des archives compressées de journaux système tous les 2 jours et purge les archives de journaux après 21 jours.

Important :
Lorsqu'un nœud est mis hors service, les fichiers journaux du nœud sont purgés immédiatement, ce qui signifie qu'ils ne sont pas archivés pendant 21 jours supplémentaires.

Vous pouvez télécharger des archives de fichiers journaux et les afficher avec **Journaux système** > **Utilités** > **Téléchargement du fichier journal de nœud**. Sélectionnez une archive de journal dans la liste, puis cliquez sur **Télécharger le journal** sous *Liens connexes pour* ouvrir ou enregistrer l'archive.

Remarque :
Les fichiers journaux ne sont disponibles que pour le nœud auquel vous êtes actuellement connecté. Pour afficher le nœud actuellement connecté, accédez à **Diagnostics du système** > **Statistiques**.

Utilisez le nouveau bouton **Afficher les enregistrements syslog** sur les formulaires Transaction et Transaction active pour afficher toutes les entrées du journal système

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

qui ont été générées lors de l'exécution de la transaction. Une transaction peut avoir n'importe quel nombre d'entrées syslog. Les multiples entrées syslog pour toutes les transactions rendent difficile la co-relation d'une transaction avec leurs entrées syslog respectives. L'action d'interface utilisateur **Afficher les enregistrements syslog** permet de mettre en relation les transactions actives et terminées avec leurs entrées syslog respectives en créant une URL pour interroger la table syslog. L'identification des entrées syslog correctes pour une transaction particulière permet de déboguer et de résoudre les problèmes de sécurité.

Sécurité de journalisation améliorée

Explorez le champ **Attribution** dans les lignes de journal du nœud pour identifier le script ou le composant qui a généré le message du journal. Les lignes de début de transaction incluent le nouveau champ pour identifier le type de demande effectuée.

Bénéficiez des résultats suivants grâce aux nouvelles améliorations :

- Retracer l'origine de chacune des lignes du journal
- Si les informations sur l'auteur ne sont pas disponibles, imprimez le nom de la classe Java et une attribution
- Au début de chaque ligne de transaction, elle contient l'ID de transaction et le type de transaction

Utilisez l'ID de transaction de chaque ligne du journal pour comprendre les informations données à chaque ligne du journal. Une fois que vous avez identifié le type de transaction, vous obtenez les informations sur l'initiateur de chaque ligne du journal. Le type de transaction et les informations sur l'origine de chaque ligne de journal vous donnent ensemble les informations sur la source requises de chaque ligne de journal de nœud.

Remarque :
SYS_UI_MACRO et SERVICE_PORTAL_WIDGET types d'écriture dans l'attribution ne sont pas indiqués.

Types de transaction

Voici la liste des types de transactions :

- Liste
- Formulaire
- XMLHttp
- Rapport
- SOAP
- Exporter
- Planificateur
- Recherche de texte
- Autre
- REST
- JSON
- AMB
- Archive

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lot REST
- Instance Scan

Propriétés système

Les propriétés système requises pour cette fonctionnalité sont les suivantes :

- Glide.log.append.attribution : cette propriété est activée par défaut. Elle active/désactive les informations d'attribution de chaque ligne de nœud
- Glide.db.log.append.classname.attribution : cette propriété est activée par défaut. Active/désactive la journalisation de l'attribution des noms de classes Java

Éviter la falsification des journaux

Configurez des règles de protection de la table de journal système pour limiter la portée de la modification et de la suppression des enregistrements du journal d'application. Les règles vous permettent de déterminer la journalisation des changements ou des tentatives de changement dans ces tables.

Si vous êtes un security_admin, activez le module d'extension Protected Tables (com.glide.protected_tables) qui permet à la plateforme de restreindre les opérations de mise à jour, d'insertion et de suppression dans les tables de journaux système suivantes :

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- protected_table_configuration (configuration non modifiable)

Remarque :
Le module d'extension com.glide.protected_tables protège uniquement les tables de journaux système mentionnées ci-dessus. Toute tentative de mise à jour, d'insertion ou de suppression d'un enregistrement enregistre un message dans la table protected_table_log.

Voir Installation et configuration du module d'extension de protection des journaux pour plus de détails.

Vous pouvez spécifier l'un des niveaux de protection des journaux suivants pour chacune des tables de journaux système.

- Bloquer et enregistrer la tentative : bloque toute modification et consigne la tentative
- Bloquer uniquement la tentative : bloque toute modification et n'enregistre pas la tentative
- Uniquement enregistrer la tentative : ne bloque pas la modification, mais consigne la tentative
- Ne pas bloquer ni journaliser la tentative : ne bloque pas la modification et ne journalise pas la tentative

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La plateforme utilise les niveaux de protection des journaux spécifiés pour chacune des tables de journaux système pour bloquer et/ou journaliser toute tentative de modification d'un enregistrement après sa création initiale.

Remarque :
Si vous êtes un security_admin, vous avez la possibilité de remplacer les niveaux de protection des journaux par défaut dans chacune des tables de journaux système pour les adapter aux personnalisations de votre instance.

Si des tentatives de modification des tables de journal système ont eu lieu, elles sont journalisées dans la table protected_table_log.

Remarque :
Si le niveau de protection n'est pas spécifié pour une table, les tentatives de modification ne sont pas enregistrées dans la table protected_table_log.

Pour désactiver les opérations de module d'extension sur les tables du Panneau d'administration, définissez la propriété com.glide.security.protected_table.enabled sur false. Voir Créer une propriété de protection du journal pour plus d'informations.

Configuration du module d'extension de protection des journaux

Configurez les règles de protection pour chaque table et opération pour terminer la configuration du module d'extension de protection des journaux.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Tables protégées** > **Protection de journal**.
   La page Panneau d'administration s'affiche.

   Remarque :
   À partir de la version Utah , le module d'extension Tables protégées est installé par défaut, mais désactivé.

2. Élevez votre rôle à security_admin afin de continuer à configurer le module d'extension.

   a. Sélectionnez **Administrateur système**.

   b. Sélectionnez **Élever le rôle**.
   Le modal Élever le rôle s'affiche.

   c. Sélectionnez l'option security_admin pour élever votre rôle, puis sélectionnez **Mettre à jour**.

3. Configurez les règles de protection pour chaque table et opération. Les règles de protection s'appliquent à la mise à jour, à l'insertion et à la suppression. Les niveaux de protection ne peuvent pas être modifiés pour certaines tables. Les tables syslog et syslog_app_scope ont des valeurs fixes pour les protections de mise à jour et de suppression. La table protected_table_configuration a des valeurs de protection fixes pour les trois opérations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour la table sysevent, les protections d'insertion ne peuvent pas être définies sur bloc.

Si **l'application aux tables enfants** était activée pour syslog dans la version précédente, les tables enfants sont ajoutées à la protection des journaux avec les mêmes règles de protection que syslog lors de la mise à niveau vers la version Utah . Cela ne se produit que pour syslog, pas pour d'autres tables.

4. Activez la fonctionnalité en sélectionnant le bouton bascule **Activer la protection du journal** .

Remarque :
Vous pouvez désactiver ce module d'extension uniquement en modifiant la propriété com.glide.security.protected_table.enabled dans la table sys_properties.

Créer une propriété de protection du journal

Créez une propriété de protection du journal pour éviter le risque d'altération du journal.

Avant de commencer
Rôle requis : admin

Procédure

1. Si la *com.glide.security.protected_table.enabled* propriété n'existe pas dans la liste Propriétés système, sélectionnez **Nouveau**.
   Le nouveau formulaire Propriétés système s'affiche.
2. Renseignez les champs du formulaire

Champs	Description
Nom	Nom de la propriété en tant que com.glide.security.protected_table.enabled
Application	Application qui possède la propriété.
Description	Description de la propriété
Choix	
Type	Type de valeur : vrai ou faux
Valeur	Valeur réelle de la propriété
Ignorer le cache	Option permettant d'ignorer le contenu du cache
Privé	Option pour rendre la propriété privée ○ Rôles de lecture ○ Rôles d'écriture

3. Sélectionnez **Soumettre** pour créer la propriété.

Connexion, audit et erreurs (sécurisation renforcée de la sécurité de l'instance)

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et agir en temps opportun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur ce qui peut être journalisé dans l'instance, reportez-vous à la section Journaux système. Assurez-vous qu'il existe un calendrier pour surveiller les événements système tels que les connexions et les échecs de connexion à l'aide de **Journaux système** > **Événements**.

Désactivation des messages d'erreur SQL (sécurisation renforcée de la sécurité de l'instance)

Utilisez cette propriété pour désactiver l'affichage `glide.db.loguser` des messages d'erreur SQL dans un navigateur.

En savoir plus

Attribut	Description
Nom de la propriété	glide.db.loguser
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l'instance	Non
Objectif	Pour désactiver l'affichage des messages d'erreur SQL dans le navigateur.
Type	true|false
Valeur recommandée	Faux
Impact fonctionnel	(Faible) Cette correction désactive le rendu des messages d'erreur SQL. Il n'y a aucun impact sur les fonctionnalités.
Risque de sécurité	(Moyen) Aucune information SQL sensible susceptible d'aider un attaquant ne doit apparaître dans le message d'erreur d'une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Gestion des secrets

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l'accès à vos mots de passe en fonction des besoins de votre entreprise.

Important :

Secrets Management a commencé son processus de fin de vie et a atteint les étapes de fin de vente et de fin de renouvellement à partir de la sortie de Yokohama. Pour prendre en charge le stockage des mots de passe avec chiffrement bidirectionnel, reportez-vous à la section Chiffrement Password2 avec Key Management Framework (KMF).

Gestion des secrets a deux versions disponibles. Secrets Management Core est inclus dans la plateforme ServiceNow sans frais supplémentaires et Secrets Management Enterprise est une version premium avec abonnement du produit. Pour plus d'informations sur la différence entre ces versions, reportez-vous à la section Explorer la gestion des secrets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les principales fonctionnalités et la valeur commerciale de Gestion des secrets.

Analyser



En savoir plus sur le tableau de bord Gestion des secrets.

Configurer



Planifiez vos configurations de base.

Traduction automatique

Explorer la gestion des secrets

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l’accès à vos mots de passe en fonction des besoins de votre entreprise.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
Les administrateurs doivent avoir le rôle d'afficher les modules et les enregistrements associés à Gestion des secrets. Pour plus d'informations sur le rôle de gestion des secrets, reportez-vous à la section Rôles de gestion des secrets.

Sélectionner parmi les versions Core et Enterprise de Gestion des secrets

Choisissez entre Secrets Management Core et Secrets Management Enterprise en fonction des besoins de votre entreprise.

Le module d'extension Gestion des secrets Core (com.glide.sm.core) est disponible par défaut. Aucune installation n'est requise sur l'instance pour l'utiliser. Le module d'extension Secrets Management Enterprise n'est disponible qu'avec une ServiceNow licence Vault v1 PROD18537. Contactez l'assistance clientèle pour obtenir de l'aide concernant le module d'extension Gestion des secrets Enterprise.

Gestion des secrets Core	Gestion des secrets d'entreprise
L'installation de Secrets Management Core sur votre instance est disponible sans frais supplémentaires. Le module d'extension permet d'utiliser des groupes de secrets avec des critères dans des tables non personnalisées fournies dans la plateforme qui ont été créées par ServiceNow les équipes d'ingénierie d'applicationServiceNow.	Gestion des secrets Enterprise inclut des fonctions supplémentaires pour aider les administrateurs à créer et à gérer des groupes de secrets. Enterprise fournit les fonctionnalités suivantes en plus des fonctionnalités répertoriées dans Core. • Utilisez des contrôles d'accès granulaires pour créer des groupes de secrets en fonction de l'un de ces critères. ◦ Champ d'application ◦ Table ◦ Colonne ◦ Enregistrement • Créez des secrets accessibles aux clients qui sont chiffrés à l'aide de votre propre clé à laquelle ServiceNow vous ne pouvez pas accéder. • Utilisez le tableau de bord de gestion des secrets pour examiner les groupes secrets configurés sur votre instance et en savoir plus sur les problèmes de sécurité potentiels. **Remarque :** Secrets Management Enterprise est un module d'extension payant que ServiceNow le personnel doit activer sur votre instance de production.

Traduction automatique

Utilisez des groupes secrets pour organiser vos secrets

Utilisez Gestion des secrets pour organiser vos secrets en groupes, puis appliquez des politiques d'accès à ces secrets au niveau du groupe.

Groupe secret de base

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces groupes s'appliquent à tous les secrets d'un périmètre. Ces secrets sont déchiffrés par un module cryptographique commun et des stratégies d'accès au module.

Groupe secret avec critères

Les groupes secrets avec critères fonctionnent de la même manière qu'un groupe secret de base, mais affinent davantage ce qui est inclus à l'aide de critères. Ces critères sont les suivants :

- Périmètre de l'application
- Package
- Table
- Colonne secrète
- Filtrer l'enregistrement

Les groupes secrets des deux types peuvent être accessibles à l'instance ou aux clients.

Groupes secrets côté instance

Les groupes secrets côté instance contiennent des secrets qui peuvent être déchiffrés par votre instance.

Groupes secrets côté client

Les groupes de secrets côté client utilisent une paire de clés publiques et privées pour s'assurer que les secrets ne peuvent être déchiffrés que par le client. Lorsque vous créez un groupe de secrets accessible au client, vous chargez la clé publique dans l'instance et conservez la clé privée sur votre serveur MID. L'instance utilise la clé publique pour chiffrer vos secrets, mais ils ne peuvent être déchiffrés qu'à l'aide de la clé privée.

Remarque :
Pour en savoir plus sur ces types de groupes, reportez-vous à la section Comprendre le côté client Gestion des secrets.

Utilisez des groupes secrets pour un contrôle plus granulaire

Bien que password2 soit disponible sur la ServiceNow plateforme, Gestion des secrets fournit ces fonctionnalités supplémentaires.

Contrôles d'accès granulaires	**Password2** Avec password2, les administrateurs peuvent contrôler l'accès à un périmètre de l'application, mais ne peuvent pas restreindre l'accès aux éléments du périmètre. **Gestion des secrets** Avec Gestion des secrets, les administrateurs peuvent restreindre l'accès en fonction des critères qu'ils définissent. Les types de critères peuvent être basés sur des critères tels que package, table ou colonne.
Stockage sécurisé	Pour les groupes secrets côté client, la gestion des secrets utilise un nouveau schéma de chiffrement. Dans ce schéma de chiffrement, ServiceNow n'enregistre pas la clé de chiffrement. Pour cette raison, la sécurité de vos données ne dépend pas de ServiceNow la sécurité.

Appliquer des politiques d'accès au module à vos groupes

Une fois que vous avez regroupé vos secrets dans un groupe secret, vous pouvez appliquer des stratégies qui déterminent comment vous pouvez y accéder au niveau du groupe. Les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

politiques d'accès aux modules sont les mécanismes de contrôle d'accès que vous appliquez aux modules cryptographiques pour définir des contrôles au niveau de l'instance, tels qu'un délai de validité de la clé cryptographique. Pour plus d'informations sur les politiques d'accès au module, voir Vue d'ensemble de la politique d'accès au module.

Tables installées avec Gestion des secrets

Gestion des secrets ajoute ou modifie ces tables.

Nouvelles tables	
[sn_sm_secret_group]	Stocke des groupes secrets
[sn_sm_secret_group_criteria]	Stocke les groupes secrets de critères
[sn_sm_secret]	Stocke les secrets enveloppés
[sn_sm_identity_group]	Définit le groupe d'identités pour le mappage d'un groupe d'identités à la clé publique
[sys_kmf_wrapped_module_key]	Stocke les clés cryptographiques symétriques encapsulées
Tables modifiées	
[sys_kmf_crypto_module]	Ajout du type de module cryptographique. (module de chiffrement d'identité ou module de chiffrement de groupe secret)
[sys_kmf_module_key]	• Stocke la clé de chiffrement secrète conceptuelle (sans matériel de clé) • Stocke la clé publique d'identité
[sys_kmf_crypto_caller_policy]	Nouveau type de politique d'accès au module ajouté

Exemples de cas d'utilisation de gestion des secrets

Garantir la sécurité de Découverte ITOM

Cette infographie présente une architecture de référence simplifiée de la façon dont ServiceNow votre organisation peut déployer IT Operations Management (ITOM) Découverte. Comme le montre l'infographie, plusieurs serveurs Windows et Linux se connectent au serveur MID (Management, Instrumentation, and Discovery) et plusieurs agents MID Server permettent le processus de détection pour mettre à jour la base de données de gestion des configurations (CMDB). Chaque transaction de serveur MID nécessite une authentification sécurisée, d'où l'importance de la gestion des informations d'identification d'authentification du point de vue de la sécurité.

Accélérer la connectivité des flux de travail avec IntegrationHub en toute sécurité

Utilisez ServiceNow le concentrateur d'intégration de pour vous connecter à différents systèmes à l'aide d'interfaces de programmation d'applications (API) automatisées. Chaque fois qu'Integration Hub se connecte à un système à l'aide d'une API, des informations d'identification d'authentification sont requises pour établir la connectivité. La gestion d'une multitude d'applications et d'API pour la connectivité nécessite une solution de gestion des secrets.

La gestion des secrets est un élément clé pour assurer la cybersécurité de votre organisation. Elle couvre tous les processus et outils liés à la création, au stockage, à la transmission et à la gestion des informations d'identification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

numériques, tels que les clés de chiffrement, les jetons d'API et les mots de passe. Pour gérer les secrets de manière sûre et efficace, vous pouvez élaborer une politique de gestion des secrets de base qui établit des règles et des procédures standard pour toutes les phases du cycle de vie d'un secret.

Comprendre le côté client Gestion des secrets

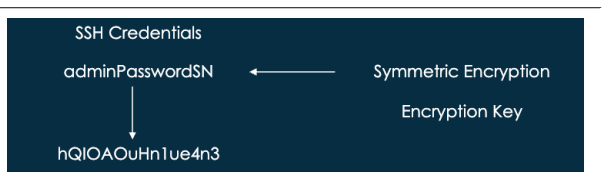
Découvrez comment gérer Gestion des secrets l'accès aux secrets et aux groupes.

Terminologie

La gestion des secrets côté client est conçue pour fournir une méthode de gestion des secrets sans l'utilisation de proxys et sans donner ServiceNow accès à vos données déchiffrées. Pour comprendre ce processus, commencez par les termes de chiffrement suivants.

Terme	Description
Chiffrement symétrique	Le chiffrement symétrique utilise une seule et même clé pour chiffrer et déchiffrer les données. Si les données sont chiffrées avec une clé symétrique, cette clé est tout ce qui est nécessaire pour les déchiffrer.
Clé symétrique	La clé symétrique chiffre un secret, transformant votre mot de passe en texte clair en texte chiffré illisible.
Chiffrement asymétrique	Le chiffrement asymétrique utilise deux clés, l'une pour le chiffrement et l'autre pour le déchiffrement.
Clé publique	La clé publique est la moitié de la paire de clés asymétrique. Cette clé est stockée sur votre instance, qui l'utilise pour chiffrer une clé symétrique. Cette clé symétrique chiffrée ne peut être déchiffrée que lorsqu'elle est associée à la clé privée.
Clé privée	La clé privée est la moitié de la paire de clés asymétrique. Cette clé est stockée dans un magasin de clés sur votre Serveur MID. ServiceNow n'a pas accès à cette clé. Combinée à la clé publique, la paire de clés asymétrique est utilisée pour déchiffrer vos secrets.

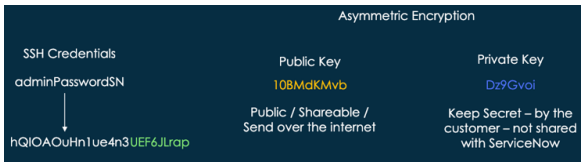
Processus de chiffrement côté client

Une clé symétrique chiffre un identifiant (dans ce cas, un mot de passe administrateur), le changeant de texte clair lisible en texte chiffré.	
La clé symétrique (représentée en vert) peut être appliquée aux informations d'identification pour les chiffrer ou les déchiffrer.	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À ce stade, le chiffrement asymétrique commence à utiliser des clés publiques (jaunes) et privées (bleues).



La clé publique chiffre les informations d'identification ainsi que la clé symétrique. La clé symétrique est maintenant protégée, elle ne peut donc pas être utilisée pour déchiffrer les informations d'identification. Bien que la clé publique puisse effectuer ce chiffrement, elle ne peut pas être utilisée seule pour déchiffrer.



Après avoir été chiffrée avec la clé publique, la clé privée est nécessaire pour déchiffrer les informations d'identification. Étant donné que le client est le seul à disposer de cette clé, il est le seul à pouvoir accéder aux informations d'identification chiffrées.



Configuration des secrets accessibles aux clients

Découvrez comment configurer votre instance pour utiliser les secrets accessibles aux clients.

Utilisez cet exemple d'implémentation pour configurer Gestion des secrets sans utiliser de proxys ni donner ServiceNow accès à vos données déchiffrées.

Pour plus de détails sur l'utilisation côté Gestion des secrets client pour gérer l'accès aux mots de passe et aux groupes, reportez-vous à la section Comprendre le côté client Gestion des secrets.

Ces instructions supposent que vous avez un serveur MID configuré sur votre réseau local. Pour plus d'informations sur ce processus, reportez-vous à la section MID Server .

Vue d'ensemble des processus

1. **Créer des clés de chiffrement et un certificat**

   Créez des clés de chiffrement et un certificat à l'aide des commandes de terminal sur votre environnement local.

2. **Ajouter votre certificat au magasin de clés de confiance ServiceNow**

   Chargez votre clé et votre certificat dans le magasin de ServiceNow clés approuvé.

3. **Créer un groupe secret avec des critères**

   Créez un groupe pour vos secrets. Groupes secrets pour organiser vos secrets en groupes. À l'aide de ces groupes, vous pouvez appliquer des politiques d'accès à ces secrets au niveau d'un groupe. Associez ensuite votre groupe de secrets à un groupe d'identités, puis ajoutez votre serveur MID à ce groupe d'identités.

4. **Charger la paire de clés publique/privée sur le serveur MID**

   Chargez votre paire de clés publique/privée sur votre serveur MID. Cette paire de clés permet au serveur MID de gérer les demandes d'authentification provenant de votre instance.

5. **Créer des informations d'identification et tester le chiffrement des informations d'identification**

   Créez des informations d'identification pour vous authentifier sur un système tiers et testez les personnes qui ServiceNow ne peuvent pas accéder aux informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. **Configurer Flow Designer pour gérer l'intégration**

   Sur votre instance, utilisez-le Studio de workflow pour gérer une intégration entre votre réseau local et votre instance.

7. **Tester l'intégration de bout en bout des secrets chiffrés côté client**

   Testez votre intégration et examinez les détails de l'exécution pour confirmer que votre configuration fonctionne.

Créer des clés de chiffrement et un certificat

Créez des clés de chiffrement et un certificat à l'aide des commandes de terminal sur votre environnement local.

Avant de commencer

Rôle requis : aucun

Procédure

1. Dans votre environnement local, ouvrez Terminal (sur Mac ou Linux) ou Ligne de commande (sous Windows).
2. À l'aide du terminal, utilisez `cd` pour vous déplacer dans le dossier où vous souhaitez stocker vos clés de cryptage.
3. À l'aide du terminal, entrez les éléments suivants :

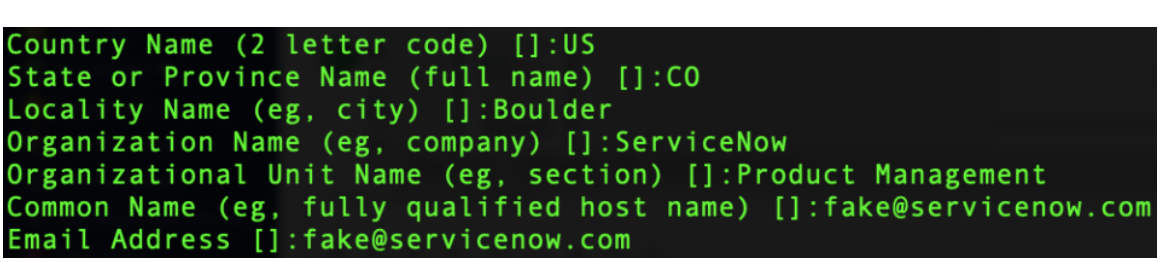
```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509 -days 365 -out
 sm_public_cert.pem
```

Remarque :
Cet exemple utilise OpenSSL pour générer des clés et des certificats. Vous pouvez remplacer d'autres outils comparables en fonction de vos besoins.

La commande génère une clé privée et un certificat public (avec la clé publique correspondante). Une série d'invites pour les informations requises suit, en commençant par « Nom du pays ».

4. Remplissez les invites avec les informations demandées.
   Les invites suivantes s'affichent.
   - Nom du pays
   - Nom de l'État de la province
   - Nom de la localité (par exemple, ville)
   - Nom de l'organisation (par exemple, société)
   - Nom de l'unité organisationnelle (p. ex., section)
   - Nom commun (par exemple, nom d'hôte complet)
   - Adresse e-mail

   Collaborez avec votre équipe de sécurité pour vous assurer que vous entrez les informations de certificat correctes.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Vérifiez le dossier que vous avez choisi à l'étape 2 pour vérifier que la clé privée et le certificat public ont été créés.
   Si vous avez utilisé les mêmes noms de fichiers que dans l'exemple de l'étape 3, vous devriez voir les fichiers suivants :
   - sm_private_key.pem
   - sm_public_cert.pem
6. Dans le même dossier, utilisez la commande suivante :

   Important :
   La commande spécifique à utiliser dépend de votre système d'exploitation.

Pour Linux :	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Pour Windows :	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

   Cette commande regroupe la clé privée et le certificat public dans un seul fichier à charger ultérieurement dans votre Serveur MID.
7. Vérifiez à nouveau le dossier pour vérifier que le nouveau fichier contenant votre clé privée (sm_keypair_bundle.pem) et votre certificat public a été créé.

Ajouter votre certificat au magasin de clés de confiance ServiceNow

Chargez votre clé et votre certificat dans le magasin de ServiceNow clés approuvé.

Avant de commencer

Rôle requis : admin

Le certificat public que vous avez créé dans cet exemple est considéré comme un certificat « autosigné » (ce qui signifie qu'il ne provient pas d'une autorité racine approuvée). Vous devez ajouter le certificat au magasin de ServiceNow clés de confiance pour qu'il soit utilisé. Lorsque vous utilisez un certificat provenant d'une autorité de certification, vous n'avez pas besoin d'effectuer cette étape.

Procédure

1. Dans votre environnement local, ouvrez Terminal (sur Mac ou Linux) ou Ligne de commande (sous Windows).
2. À l'aide du terminal, utilisez `cd` pour accéder au dossier où vous avez créé vos clés de chiffrement.
3. Dans le terminal, entrez la commande suivante :

   ```
   cat sm_public_cert.pem
   ```

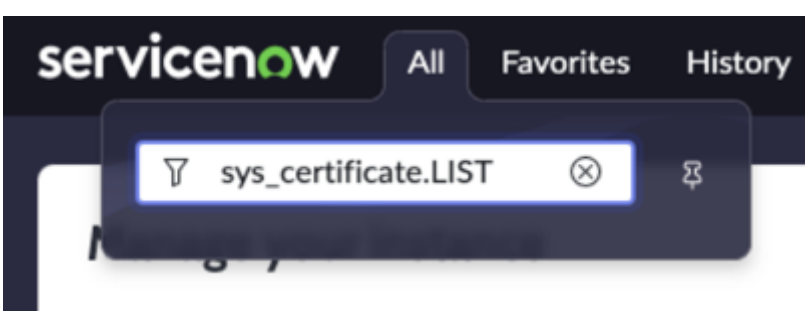
   Vous devez afficher le contenu de votre certificat public pour le copier dans le magasin de clés approuvé. Cette commande `cat` affiche le certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Copiez les informations du certificat dans le presse-papiers.
   Commencez par la ligne `-----BEGIN CERTIFICATE -----` et incluez la ligne `-----END CERTIFICATE -----` et incluez-la.
5. Sur votre ServiceNow instance, accédez à la liste des **certificats X.509** en saisissant `sys_certificate.LIST` dans le filtre de navigation.



6. Sélectionnez **Nouveau** pour créer un enregistrement de **certificat X.509** .
7. Dans le formulaire, renseignez les champs suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du certificat X.509

Champ	Valeur
Nom	Nom du certificat. Ce nom peut être n'importe quel nom de votre choix.
Format	Sélectionner **PEM** **Remarque :** Les fichiers PEM (Privacy Enhanced Mail) sont un type de fichier d'infrastructure à clé publique (PKI) utilisé pour les clés et les certificats. Les enregistrements que vous avez créés aux étapes précédentes sont de ce type de fichier.
Type	Sélectionner **le certificat de magasin de confiance**
Description brève	Description du certificat. Entrez une valeur qui vous indique l'utilité de ce certificat.
Certificat PEM	Collez les informations de certificat que vous avez copiées à l'étape 4.

8. Sélectionnez **Soumettre** pour sauvegarder l'enregistrement.

Créer un groupe secret avec des critères

Créez un groupe pour vos secrets. Groupes secrets pour organiser vos secrets en groupes et vous permettre d'appliquer des politiques d'accès à ces secrets au niveau du groupe. Associez ensuite votre groupe de secrets à un groupe d'identités, puis ajoutez votre serveur MID à ce groupe d'identités.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Gestion des secrets** > **Groupes secrets avec critères**.
2. Sélectionnez **Nouveau** pour créer un **groupe secret avec un enregistrement de critères** .
3. Dans le formulaire, renseignez les champs suivants.

Groupe secret avec champs de critères

Champ	Valeur
Nom du groupe	Nom du groupe secret. Ce nom peut être n'importe quel nom de votre choix.
Type de secret	Sélectionner **Accessible au client**
Module de génération automatique	Cochez la case

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Description brève	Description du groupe secret. Entrez une valeur qui indique l'utilité de ce groupe.
Type de critère	**Sélectionner une table cible**
Table cible	**Sélectionner les informations d'identification SSH [ssh_credentials]**

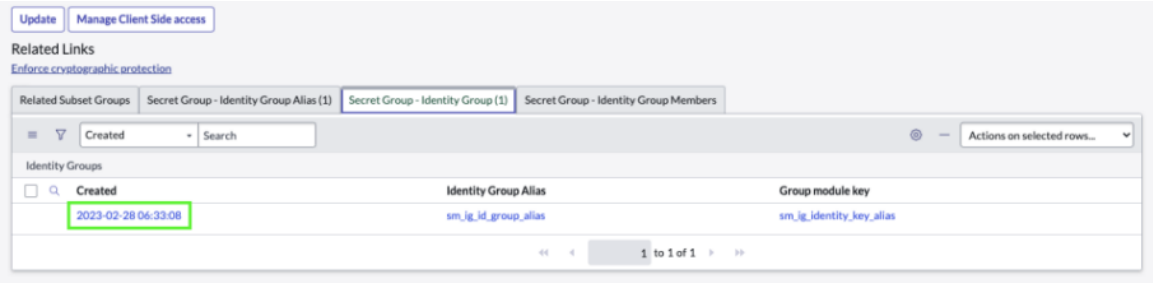
4. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) sur l'en-tête du formulaire, puis sélectionnez **Enregistrer** dans le menu contextuel pour enregistrer l'enregistrement.
5. Assurez-vous que la case **Actif** n'est pas cochée.
6. Sélectionnez le bouton **Gérer l'accès côté client** pour créer un groupe d'identités.
   Une fenêtre **d'alias de groupe d'identités** s'affiche.
7. Sélectionnez le bouton **Nouveau** .
8. Sélectionnez l'icône de référence ( ) en regard du champ **Alias du groupe d'identités** .
9. Dans le champ **Nom de l'alias du groupe** , entrez une valeur.
   Ce nom peut être la valeur que vous voulez.
10. Si vous avez choisi un nom unique à l'étape 9, sélectionnez **Soumettre**.
11. Sélectionnez le bouton **Télécharger la clé d'identité** .
    La fenêtre **Importer le certificat de clé publique d'identité** s'affiche.
12. Dans le champ **Alias de clé d'identité** , saisissez une valeur.

> **Important :**
> Cette valeur peut être ce que vous voulez, mais elle doit correspondre exactement à ce que vous insérez ultérieurement dans le serveur MID.

13. **Sélectionner Importer**
    La fenêtre **Pièce jointe** s'affiche.
14. Sélectionnez **Choisir un fichier**.
15. Sélectionnez le certificat public que vous avez créé lors des étapes précédentes.
    Ce certificat doit être le fichier `sm_public_cert.pem` .
16. Sélectionnez l'icône X pour fermer la fenêtre.
17. Sélectionnez **OK** pour fermer la fenêtre **Importer le certificat de clé publique d'identité** .
    Une bannière bleue **Les clés et les certificats sont importés avec succès dans l'instance et s'affiche** pour confirmer la réussite de l'importation.
18. Sélectionnez **Soumettre**.
    La liste **Groupes d'identité** s'affiche.
19. Cochez la case à gauche de votre enregistrement de groupe d'identités dans la liste.
20. Sélectionnez le bouton **Associer un groupe secret** .
    Vous êtes renvoyé à votre **groupe secret avec l'enregistrement Critères** . Les listes connexes **Groupe secret – Alias du groupe d'identités** et **Groupe secret – Groupe d'identités** sont visibles. Ces listes connexes affichent les enregistrements que vous avez créés lors des étapes précédentes.
21. Dans la liste connexe **Groupe secret – Groupe d'identités** , sélectionnez le champ **Créé** pour l'enregistrement de cette liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un enregistrement **de groupe d'identité** s'affiche.

22. Dans la liste connexe **Membres du groupe d'identité** , sélectionnez le bouton **Nouveau** .
Un enregistrement **de membre du groupe d'identités** s'affiche.
23. Dans le champ **Table des membres**, sélectionnez **Serveur MID [ecc_agent].**
24. Sélectionnez l'icône de référence ( ) en regard du champ d'enregistrement Membre du **groupe d'identité** , puis sélectionnez votre serveur MID.

> **Remarque :**
> Si vous cochez la case **Inclure tous les enregistrements** , tous les serveurs MID connectés à votre instance sont ajoutés au groupe d'identités.

25. Sélectionnez **OK** pour fermer la fenêtre **Sélectionner le document** .
26. Sélectionnez **Soumettre**.
27. Revenir à **Tous** > **Gestion des secrets** > **Groupes secrets avec critères**et ouvrez l'enregistrement que vous avez créé à l'étape 2.
28. Activez le champ **Actif** .
29. Sélectionnez **Mettre à jour** pour sauvegarder l'enregistrement.

Charger la paire de clés publique/privée sur le serveur MID

Chargez votre paire de clés publique/privée sur votre serveur MID. Cette paire de clés permet au serveur MID de gérer les demandes d'authentification provenant de votre instance.

Avant de commencer

Rôle requis : aucun

Étant donné ServiceNow qu'il n'a pas accès à la clé privée, il ne peut pas l'associer à la clé publique pour déchiffrer la clé symétrique, puis déchiffrer les informations d'identification. Si le serveur MID tente d'utiliser ces informations d'identification chiffrées, il ne parvient pas à déchiffrer les informations d'identification à des fins d'authentification sans accès à la clé privée.

Au cours de ces étapes, vous chargez la clé privée sur le serveur MID pour terminer le trousseau public/privé. Ce chargement accorde l'accès au serveur MID sans donner ServiceNow d'accès.

Pour accorder au Serveur MID l'accès à la clé privée, vous devez élaborer une commande à exécuter en tant qu'administrateur dans PowerShell. Dans cet exemple, la commande est destinée à l'ordinateur virtuel Windows Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

Assurez-vous que le système sur lequel vous effectuez ces étapes a accès à la fois au serveur MID et au fichier de la paire de clés.

Procédure

1. Dans votre environnement local, localisez le dossier dans lequel vous avez Créer des clés de chiffrement et un certificat créé votre paire de clés.
2. Recherchez et copiez le chemin d'accès complet au fichier `manage-certificates.bat` .

   Remarque :
   Ce fichier se trouve dans votre dossier Serveur MID. Selon l'endroit où vous avez stocké votre dossier Serveur MID, votre chemin d'accès peut ressembler à cet exemple :

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__
   patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manag
   e-certificates.bat
   ```

3. Créez un fichier texte et collez-le dans le fichier.
4. Dans le fichier texte, ajoutez ce qui suit après le chemin d'accès :
   `-un your_identity_key_alias`

   Remplacez `your_identity_key_alias` par le nom de l'alias de clé d'identité que vous avez créé lors du chargement de votre certificat public.
5. Recherchez et copiez le chemin d'accès complet à votre fichier de paire de clés.

   Remarque :
   Si vous avez utilisé les noms dans ces étapes, ce fichier est nommé `sm_keypair_bundle.pem`.

6. Dans votre fichier texte, ajoutez ce chemin à la fin de la ligne, en ajoutant un espace entre ce chemin et les informations précédentes.
   Le texte de votre fichier texte doit ressembler à cet exemple :

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch
   4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificat
   es.bat -a your_identity_key_alias
    C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
   ```

   Remarque :
   Dans cet exemple, le fichier `sm_keypair_bundle.pem` se trouve sur le bureau pour raccourcir le chemin.

7. Copiez l'intégralité du texte de votre fichier texte dans le presse-papiers.
8. Recherchez Powershell sur votre système, puis choisissez l'option **Exécuter en tant qu'administrateur** .
9. Collez le texte de votre fichier texte dans PowerShell, puis appuyez sur Entrée.
   En cas de réussite, le message suivant s'affiche :

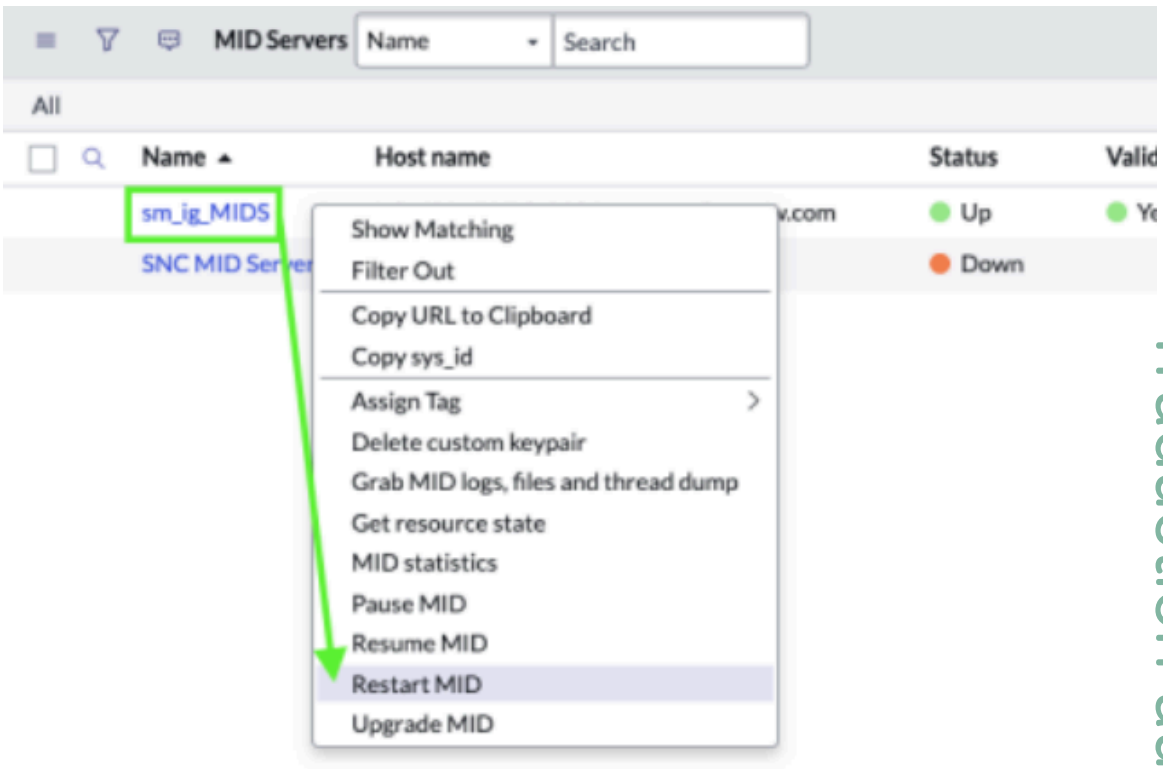
   ```
   Installed certificate with alias: <your_identity_key_alias> into the MID keystore.
   ```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :
Si vous ne voyez pas ce message, assurez-vous que votre commande ne contient pas d'erreurs, d'espaces ou de guillemets inutiles. Assurez-vous que le chemin d'accès complet est saisi correctement.

10. Redémarrez votre Serveur MID en accédant à votre enregistrement de Serveur MID, en cliquant dessus avec le bouton droit de la souris et en sélectionnant **Redémarrer le MID.**



Le redémarrage du serveur MID synchronise la paire de clés chargée dans le magasin de clés MID pour une utilisation avec des opérations. Attendez le redémarrage du Serveur MID avec l'état **Actif** et la valeur validée **Oui** avant de continuer.

Créer des informations d'identification et tester le chiffrement des informations d'identification

Créez des informations d'identification à authentifier dans un système tiers.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

Important :
L'utilisateur connecté du serveur MID doit également avoir les rôles suivants : administrateur, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la liste **des informations d'identification SSH** en saisissant `ssh_credentials.list` dans le filtre de navigation.
2. Sélectionnez **Nouveau** pour créer un enregistrement **d'informations d'identification SSH** .
3. Dans le formulaire, renseignez les champs suivants.

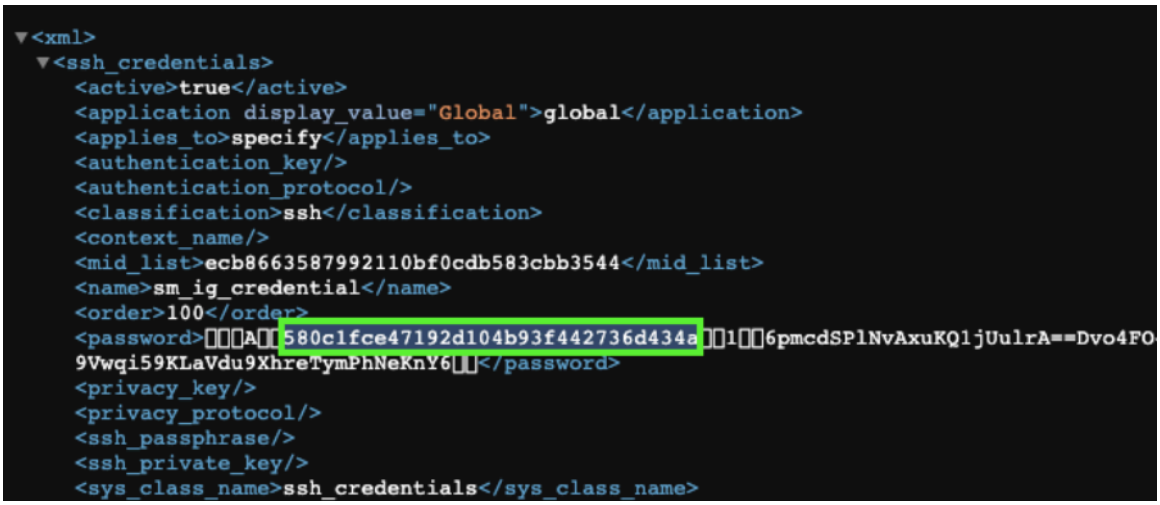
Formulaire d'informations d'identification SSH

Champ	Valeur
Nom	Entrez un nom pour votre enregistrement d'informations d'identification. Ce nom peut être la valeur que vous voulez.
Concerne	**Sélectionner des serveurs MID spécifiques**
Serveurs MID	Sélectionnez votre Serveur MID.
Nom d'utilisateur	Entrez le nom d'utilisateur.
Mot de passe	Entrez le mot de passe associé à l'utilisateur dans le champ **Nom d'utilisateur** .

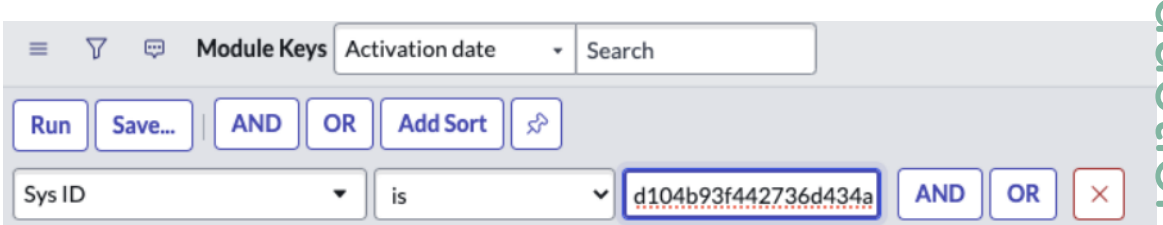
4. Sélectionnez l'icône de verrouillage ( ) en regard du champ **Alias d'informations d'identification** .
5. Sélectionnez l'icône de référence ( ) pour ouvrir la liste des **alias de connexion et d'informations d'identification** .
6. Sélectionnez **Nouveau** pour créer un enregistrement **d'alias de connexion et d'informations d'identification** .
7. Entrez un nom dans le champ **Nom** .
8. Sélectionnez **Informations d'identification** dans le champ **Type** .
9. Sélectionnez **Soumettre**.
   Vous êtes renvoyé à l'enregistrement des **informations d'identification SSH** . Dans les étapes suivantes, vous testez que les informations d'identification sont chiffrées.
10. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) sur l'en-tête du formulaire et sélectionnez **Afficher le code XML**.
11. Recherchez la balise XML `<password>` dans le code XML.
12. Copiez les sys_id de cette balise `<mot de passe>` dans votre presse-papier.
    Le sys_id est un code de 32 caractères représentant la clé symétrique utilisée pour chiffrer ces informations d'identification. Le mot de passe chiffré que vous avez saisi dans la table Informations d'identification SSH se trouve à droite des deux ensembles de cases sur cette même ligne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



13. Accédez à la liste des **clés de module** en saisissant sys_kmf_module_key.list dans le filtre de navigation.
14. Filtrez la liste des enregistrements dans lesquels le champ **ID système** correspond à l'sys_id que vous avez copié à l'étape 12, puis sélectionnez **Exécuter**.



Votre recherche doit renvoyer un seul enregistrement de **clé de module** . Cet enregistrement vous montre que vous avez créé avec succès une clé symétrique et que vous l'utilisez.

15. Accédez à la liste **des clés de module encapsulées** en saisissant sys_kmf_wrapped_module_key.list dans le filtre de navigation.
16. Filtrez la liste des enregistrements dans lesquels le champ **Module de chiffrement** correspond au module de chiffrement que vous avez créé dans les étapes précédentes, puis sélectionnez **Exécuter**.
Votre recherche doit renvoyer un seul enregistrement **de clé de module encapsulée** . Dans cette liste, vous pouvez vérifier les points suivants :
    - La colonne **de matériel de clé encapsulée** montre que la clé symétrique dans le module de chiffrement (qui est utilisée pour chiffrer les informations d'identification SSH) est chiffrée par la clé publique que vous avez téléchargée dans le groupe d'identités.
    - Le champ ID système de **clé encapsulée** montre que c'est la clé (la clé symétrique du module de chiffrement) qui est chiffrée par l'ID système de clé **d'encapsulation** (la clé publique chargée dans le groupe d'identités).

Si les champs précédents ne figurent pas sur votre liste par défaut, vous pouvez les ajouter à la liste en sélectionnant l'icône **Personnaliser la liste** (bouton Personnaliser la).

Remarque :
Votre instance exécute une tâche de nettoyage toutes les 10 minutes, ce qui supprime les clés orphelines et empêche la prolifération de clés non associées après la mise à jour de vos informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Flow Designer pour gérer l'intégration

Sur votre instance, utilisez-le Studio de workflow pour gérer une intégration entre votre réseau local et votre instance.

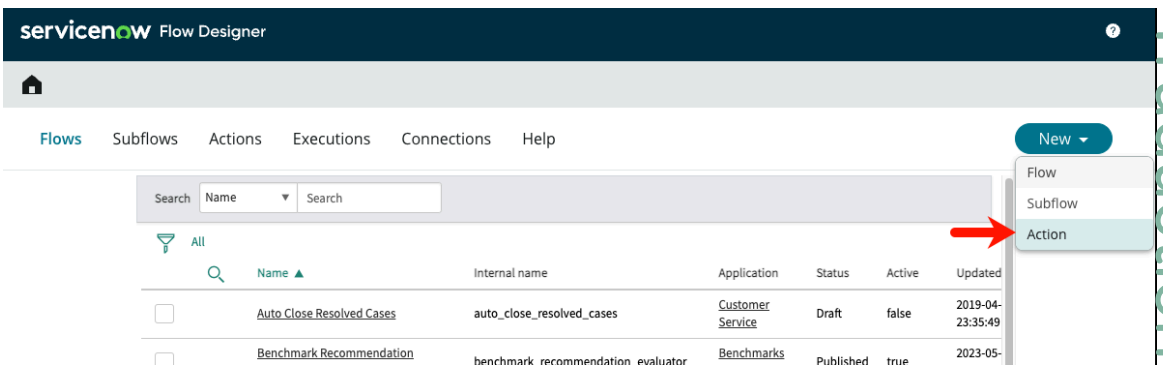
Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

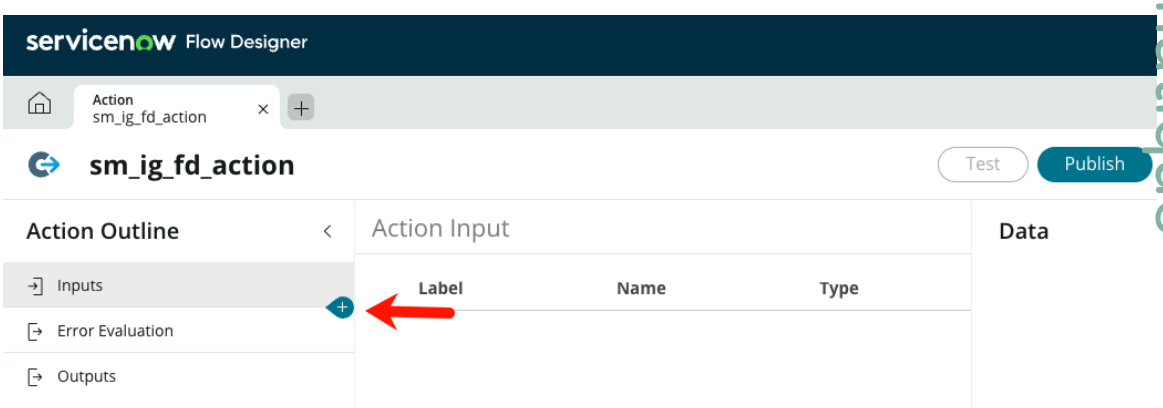
Au cours de ces étapes, vous créez un Studio de workflow workflow pour créer un fichier texte sur votre système local.

Procédure

1. Sur votre instance, accédez à **Tous** > **Automatisation des processus** > **Concepteur de flux**.
2. Créez une action dans ServiceNow en sélectionnant **Nouveau** et **Action**.



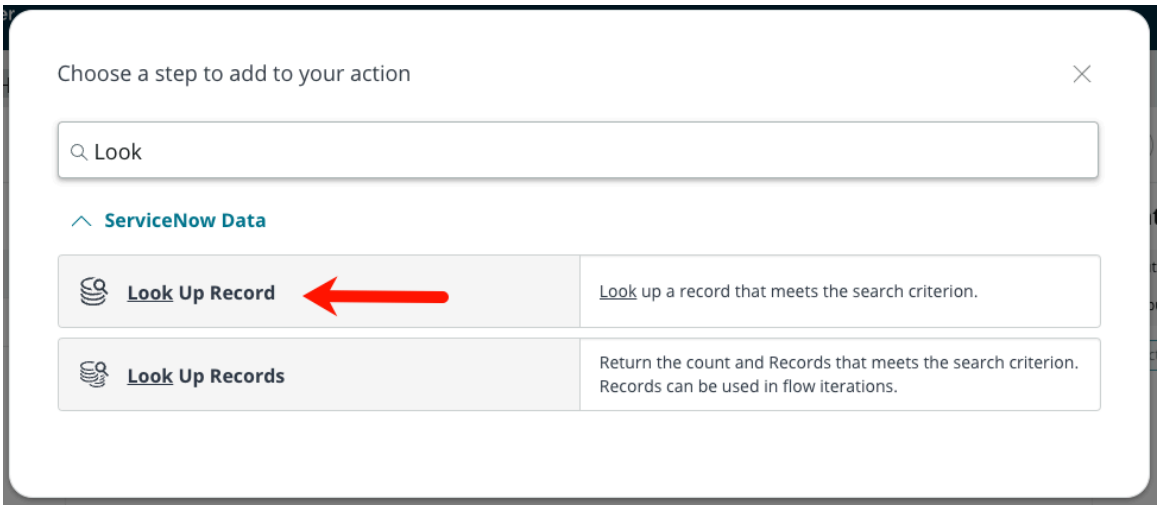
3. Entrez un nom dans le champ **Nom de l'action** , puis sélectionnez **Soumettre**.
4. Créez une étape en sélectionnant le signe plus entre **Entrées** et Évaluation des erreurs dans le **Plan d'action**.



5. Dans la fenêtre **Choisir une étape à ajouter à votre fenêtre d'action** , sélectionnez **Rechercher un enregistrement**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



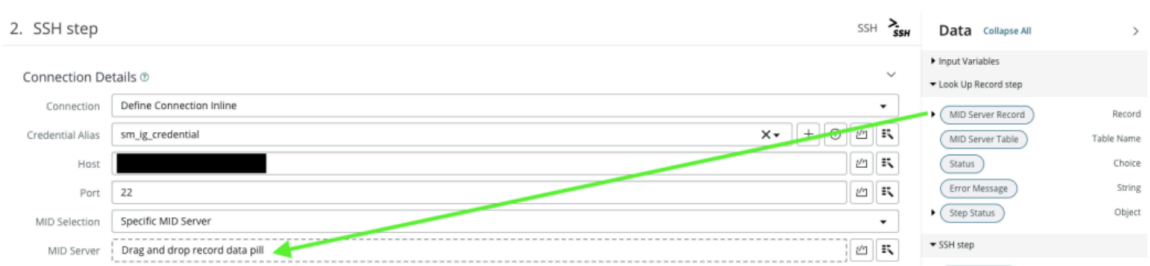
6. Dans la section Étape **Rechercher un enregistrement** , sélectionnez **Serveur MID [ecc_agent]** dans le champ **Table** .
7. Créez une autre étape en sélectionnant le signe plus sous votre **étape Rechercher un enregistrement**.
8. Dans la fenêtre **Choisir une étape à ajouter à votre fenêtre d'action** , sélectionnez **SSH**.

> **Remarque :**
> Si vous ne voyez pas l'option **SSH** , vous devez activer le module d'extension requis.

9. Dans la section **Étape SSH** , saisissez les informations suivantes :

Champ	Valeur
Connexion	**Sélectionner Définir l'inline de la connexion**
Alias d'informations d'identification	Sélectionnez l'alias d'informations d'identification des informations d'identification SSH créées lors des étapes précédentes.
Hôte	Entrez l'adresse IP de l'hôte auquel vous vous connectez via SSH.
Port	Entrez 22.
Sélection de MID	Sélectionner **un serveur MID spécifique**.

10. Pour remplir le champ de **Serveur MID** , faites glisser la pastille **d'enregistrement de Serveur MID** de la section **Données** vers le champ.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Lorsque vous faites glisser la pastille dans le champ, sélectionnez la pastille et non la flèche noire à côté de la pastille.

11. Dans la section **Configuration SSH** , entrez la valeur suivante dans le champ **Commande** .

```
/bin/date > sm_ig_text_file.txt
```

Cette commande crée un fichier texte dans votre système local à l'aide des secrets déchiffrés du Serveur MID. Le serveur MID accorde l'accès à l'instance ServiceNow (via Studio de workflow) sans jamais donner à l'instance ServiceNow l'accès au secret déchiffré.

Conseil :
La commande `/bin/date` insère la date/heure actuelle dans le fichier texte créé. Cette commande montre que l'intégration se produit en temps réel en fonction de la date/heure actuelle par rapport à la date de création du fichier texte.

12. Sélectionnez le bouton **Enregistrer** pour enregistrer le workflow.

Tester l'intégration de bout en bout des secrets chiffrés côté client

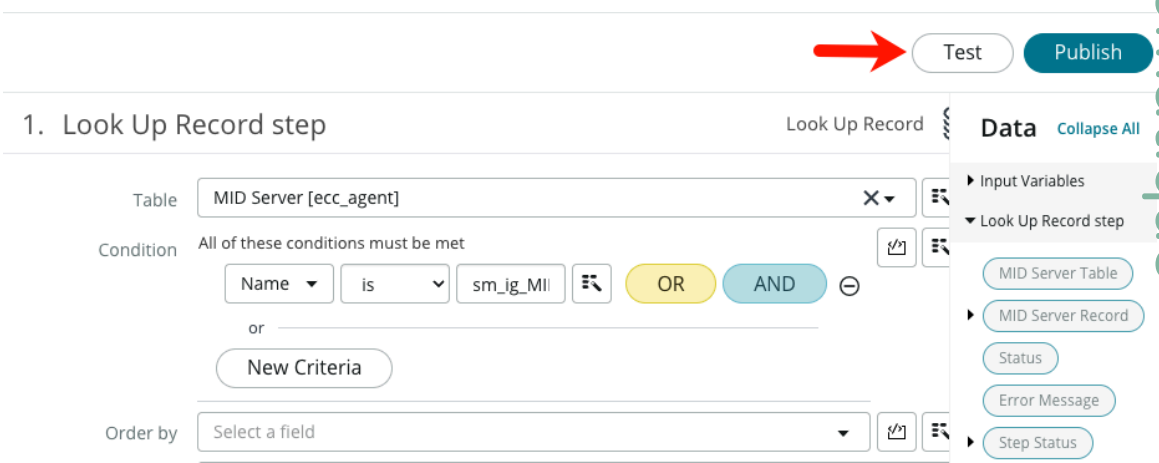
Testez votre intégration et examinez les détails de l'exécution pour confirmer que votre configuration fonctionne.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

Procédure

1. Dans Studio de workflow , sélectionnez le bouton **Test** dans le coin supérieur droit de l'écran.



2. Dans la fenêtre **Action de test** , sélectionnez **Exécuter le test**.

3. Sélectionnez **L'exécution de votre test terminée. Affichez les détails d'exécution de l'action.**

4. Actualisez votre écran jusqu'à ce que vous voyiez **Exécution du test - Terminé** en haut à droite de l'écran.

5. Sélectionnez la flèche **Étapes** en bas à gauche de l'écran.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Faites défiler vers le bas jusqu'à ce que vous voyiez un en-tête **de données de sortie d'étape** avec le message de réussite suivant :

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Après avoir vu ce message dans Studio de workflow, vérifiez que votre fichier texte a été créé dans votre système local.

Tester une information d'identification Windows Management Instrumentation chiffrée avec Gestion des secrets

Vérifiez que vos informations d'identification WMI (Windows Management Instrumentation) sont chiffrées avec Gestion des secrets et utilisez un workflow IntegrationHub pour terminer les tests de bout en bout.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

- Le concentrateur d'intégration Enterprise doit être actif sur votre instance. Pour plus de détails, voir Request an Integration Hub plugin .
- Vous devez disposer d'un groupe de secrets configuré sur votre instance. Voir les étapes 1 à 3 énumérées dans .Configuration des secrets accessibles aux clients
- Vous devez disposer d'informations d'identification configurées chiffrées avec Gestion des secrets. Voir les étapes 1 à 9 énumérées dans .Créer des informations d'identification et tester le chiffrement des informations d'identification

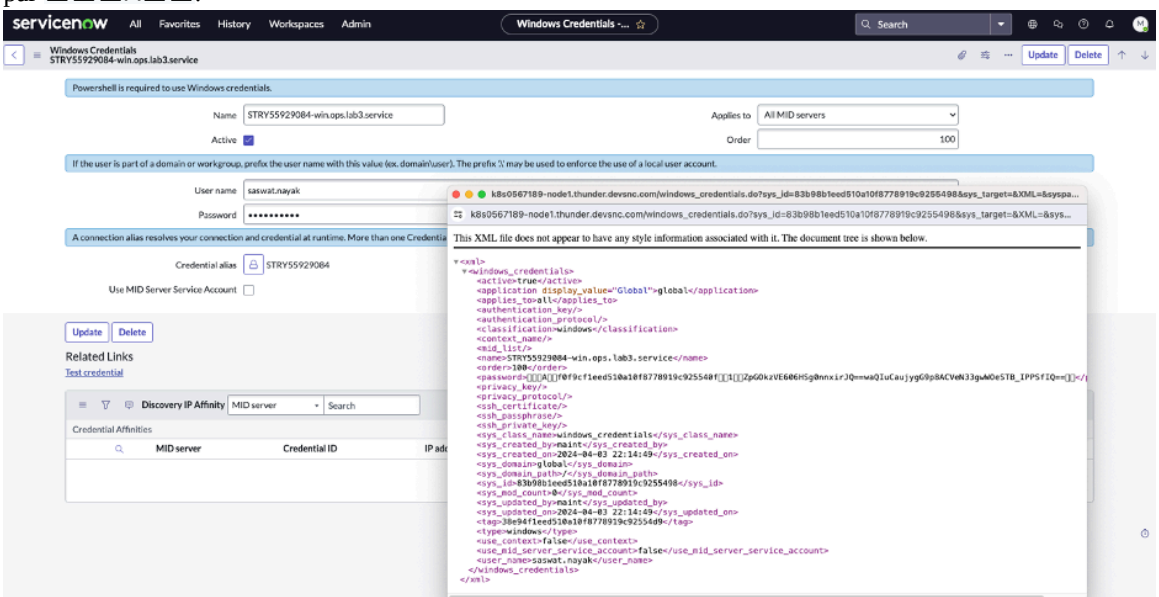
Procédure

1. Confirmez que le serveur MID souhaité est associé au groupe secret.
   Ouvrez l'enregistrement Groupe secret avec critères [sn_sm_criteria_secret_group] et recherchez votre serveur MID dans la liste **Groupe secret – Membres du groupe d'identités** . Si votre serveur MID n'est associé à aucun groupe, reportez-vous à la section Créer un groupe secret avec des critères.
2. Confirmez que les informations d'identification sont chiffrées avec Gestion des secrets.
   a. Accédez à la **Tous** > **Centre d'intégration** > **Connexions et informations d'identification** > **Informations d'identification**.
   b. Ouvrez votre enregistrement d'informations d'identification.
   Vérifiez qu'un alias d'informations d'identification est répertorié dans le champ **Alias d'informations d'identification** . Si vous n'en avez pas encore créé, reportez-vous à la section Créer un alias de connexion et d'informations d'identification.
   c. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête de votre enregistrement d'informations d'identification, puis sélectionnez **Afficher le code XML** dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Dans la vue XML de l'enregistrement, recherchez le mot de passe et confirmez que la valeur commence par □□□A□□.



3. Créez un workflow de test dans Studio de workflow.

a. Accédez à la **Tous** > **Automatisation des processus** > **Studio de workflow**.

b. Sélectionnez **Nouveau**, **puis Action dans** la liste.

c. Entrez un nom dans le champ **Nom de l'action** .
Laissez le champ **Application** défini sur Global.

d. Sélectionnez le bouton **d'action Créer** .

4. Configurez une étape de recherche d'enregistrement dans Studio de workflow.

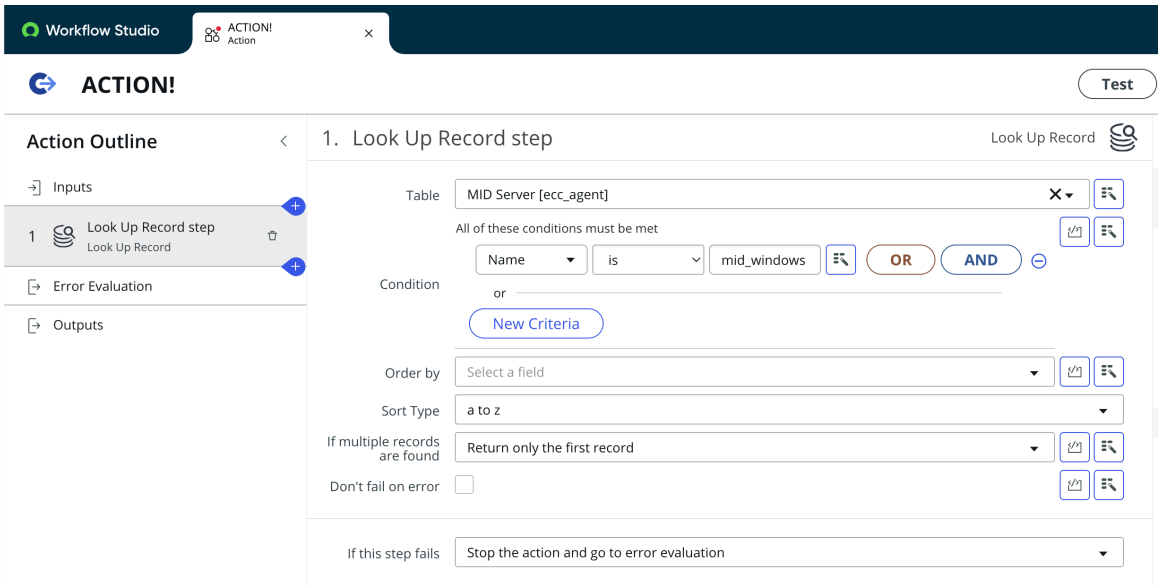
a. Dans Plan **d'action**, sélectionnez le bouton Plus pour ajouter une nouvelle étape.
Recherchez et sélectionnez le type d'étape **Rechercher un enregistrement** .

b. Dans le champ **Table**, sélectionnez **Serveur MID [ecc_agent].**

c. Pour la condition, sélectionnez **Nom est**, suivi du nom de votre Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Important :
Assurez-vous que le Serveur MID sélectionné est le même que celui associé au groupe secret.

5. Configurez une étape de recherche d'enregistrement dans Studio de workflow.

a. Dans Plan **d'action**, sélectionnez le bouton Plus pour ajouter une nouvelle étape sous votre étape Rechercher un enregistrement.
Recherchez et sélectionnez le type d'étape **PowerShell** .

b. Dans le formulaire **Étape PowerShell** , renseignez les champs selon vos besoins.

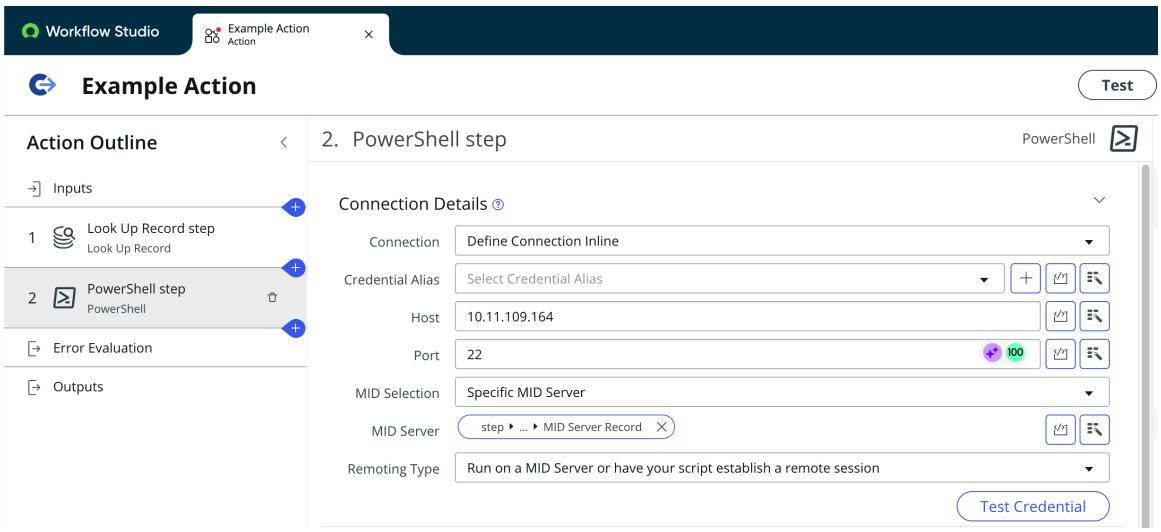
Champs d'étapes PowerShell

Champ	Valeur
Connexion	**Sélectionner Définir l'inline de la connexion**
Alias d'informations d'identification	Sélectionnez votre alias d'informations d'identification
Hôte	Entrez l'adresse IP du serveur Windows cible
Port	Entrez 22 s'il ne s'agit pas déjà de la valeur par défaut.
Sélection de MID	Sélectionnez **MID Server spécifique**
Serveur MID	Faire glisser la pastille **d'enregistrement de Serveur MID** à partir du panneau **de données** Cette pastille de données est visible dans le panneau **Données** sur le bord droit de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	l'écran, sous **l'étape Rechercher une étape d'enregistrement**.
Type d'accès à distance	Sélectionnez **Exécuter sur un serveur MID ou demandez à votre script d'établir une session à distance**



6. Créez un script pour votre action de test.

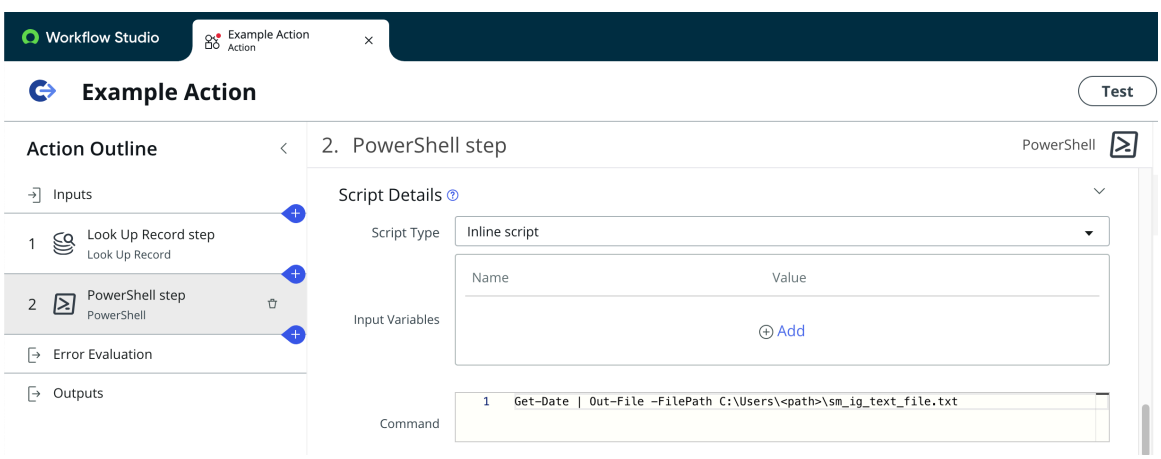
a. Dans le champ **Type de script** , sélectionnez **Script en ligne**.

b. Utilisez le script suivant, en remplaçant l'exemple de chemin d'accès par le chemin d'accès de votre hôte de test.

```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

Remarque :
Vous pouvez également exécuter votre propre script qui convient à la configuration de votre hôte distant. Il est important de confirmer qu'une connexion a été établie à l'aide de la valeur chiffrée SM.

c. Sélectionnez le bouton **Enregistrer** pour enregistrer votre action.

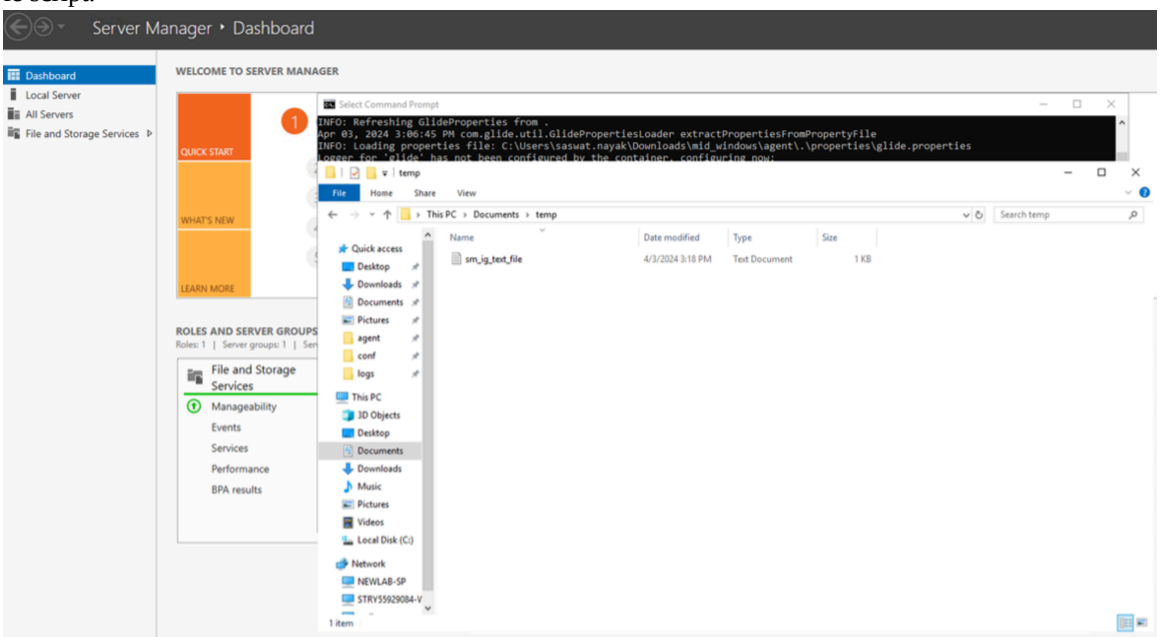


7. Sélectionnez le bouton **Test** pour tester votre action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Examinez les journaux de sortie pour détecter tout message d'erreur.
9. Vérifiez qu'un fichier de test a été créé sur le serveur hôte dans le chemin d'accès que vous avez fourni dans le script.



Clonage et gestion des secrets

Découvrez comment reconfigurer des groupes de secrets et des groupes de secrets clients après un clone.

Après avoir cloné une instance, vos groupes de secrets et vos groupes de secrets clients devront peut-être être reconfigurés pour fonctionner comme prévu.

Origine du groupe de clés secrètes	Comportement après un clone
Groupes secrets de l'instance d'origine à partir de l'instance cible	Fonctionne comme prévu après importation manuelle du module de chiffrement manquant. Consultez Exporting and importing data via XML .
Groupes de secrets clients d'origine de l'instance cible	Fonctionne comme prévu après importation manuelle du module de chiffrement manquant. Consultez Exporting and importing data via XML .
Groupes de secrets d'instance clonés à partir de l'instance source	Ne fonctionne pas à moins d'être configuré manuellement
Groupes de secrets clients clonés à partir de l'instance source	Travailler si configuration manuelle sg/identity group/ alias/mid

Tableau de bord de gestion des secrets

Utilisez le tableau de bord de gestion des secrets pour examiner les groupes secrets configurés sur votre instance et pour en savoir plus sur les problèmes de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du groupe secret



L'onglet **Vue d'ensemble du groupe secret** affiche des informations sur vos groupes secrets configurés. Utilisez cet onglet pour afficher des informations sur les groupes de secrets configurés sur votre instance.

Groupe secret par type

Affiche un graphique à secteurs présentant les groupes secrets installés sur votre instance, regroupés par type de secret (côté instance côté client).

Groupe secret par type de critère

Affiche un graphique à secteurs présentant les groupes secrets avec des critères configurés sur votre instance par le type de critère utilisé.

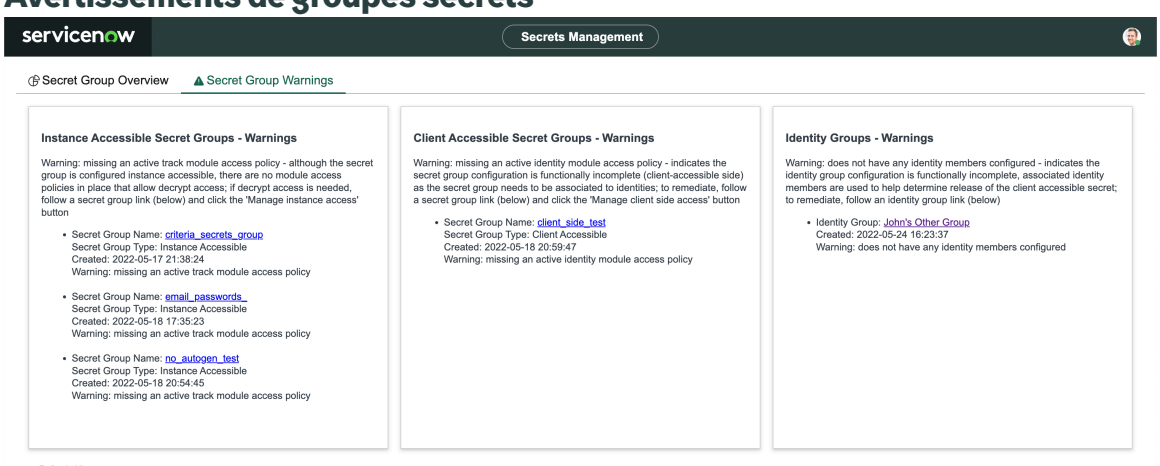
Nombre de groupes de secrets inactifs

Affiche le nombre de groupes secrets inactifs configurés sur votre instance.

Nombre de secrets dédiés

Affiche le nombre de secrets au sein des groupes secrets de base.

Avertissements de groupes secrets



L'onglet **Avertissements de groupes secrets** affiche les avertissements relatifs à vos groupes secrets et groupes d'identités.

Groupes secrets accessibles aux clients - Avertissements

Cette carte affiche des avertissements s'il existe des groupes secrets sans politique d'accès active en place. Sélectionnez un nom de groupe secret pour afficher cet enregistrement.

Groupes secrets accessibles aux clients - Avertissements

Cette carte affiche des avertissements s'il existe des groupes secrets accessibles aux clients qui n'ont pas de politique d'accès au module d'identité (MAP) active. Sélectionnez un nom de groupe secret pour afficher cet enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupes d'identité - Avertissements

Cette carte affiche des avertissements s'il existe des groupes d'identités pour lesquels aucun membre n'est configuré. Sélectionnez le nom du groupe d'identités pour afficher l'enregistrement.

Remarque :
Le tableau de bord Gestion des secrets fait partie de Secrets Management Enterprise. Secrets Management Enterprise est un module d'extension payant que ServiceNow le personnel doit activer sur votre instance de production.

Rôles de gestion des secrets

La gestion des secrets ajoute ces rôles.

Administrateur des secrets [sn_secrets.admin]

Affectez des rôles de secrets non administrateurs à d'autres utilisateurs. Les administrateurs de secrets disposent des mêmes privilèges que le gestionnaire de secrets et le visualiseur.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Important :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

- Un utilisateur doit avoir à la fois les rôles administrateur et security_admin pour se voir affecter le rôle sn_secret.admin.
- Évitez d'accorder un rôle d'administrateur lorsque des rôles plus ciblés sont disponibles.

Gestionnaire de secrets [sn_secrets.secret_manager]

Accordez ce rôle aux utilisateurs qui doivent être en mesure d'exécuter l'une des fonctions suivantes.

- Afficher les enregistrements secrets et de groupes secrets
- Afficher l'historique d'accès et d'autres informations sur les activités d'utilisation
- Créer des groupes et des filtres secrets
- Créer des fournisseurs secrets
- Déplacer les secrets entre les groupes secrets
- Modifier les paramètres du groupe secret et du fournisseur secret

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Important :
Les gestionnaires de secrets ne peuvent pas voir les secrets en texte brut.

Visionneuse de secrets [sn_secrets.viewer]

Accordez ce rôle aux utilisateurs qui doivent être en mesure d'afficher des enregistrements secrets et des groupes secrets.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Aucun.

Créer un module cryptographique de groupe secret

Créez un module cryptographique de groupe secret pour effectuer le chiffrement et le déchiffrement.

Avant de commencer

Rôle requis :

- administrateur
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

Procédure

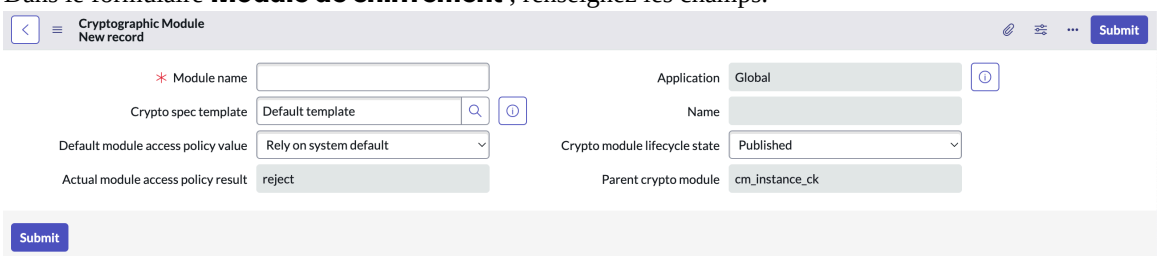
1. Accédez à la **Tous** > **Gestion des secrets** > **Créer un module de chiffrement de groupe secret**.
2. Sélectionnez le type de module de chiffrement de groupe que vous souhaitez créer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de module de chiffrement	Description
Créer un module de chiffrement secret accessible à l'instance	Créez des secrets accessibles à l'instance qui peuvent être déchiffrés par votre instance.
Créer un module de chiffrement secret accessible aux clients	Créez des secrets accessibles aux clients qui sont chiffrés à l'aide de votre propre clé, qui ServiceNow ne peut pas accéder.

3. Dans le formulaire **Module de chiffrement** , renseignez les champs.



Champ	Description
Nom du module	Nom descriptif pour votre module
Application	Le périmètre de l'application qui contient votre module. Ce champ est automatiquement renseigné avec le module actuel.
Modèle de spécification de chiffrement	**Le modèle par défaut** est sélectionné par défaut.
Nom	Nom du module. Ce nom est généré automatiquement en fonction du nom de l'application et du module.
Valeur de la politique d'accès au module par défaut	○ S'appuyer sur le système par défaut ○ Refuser ○ Trace
État du cycle de vie du module de chiffrement	Indique si le module est à l'état **Brouillon** ou **Publié** .
Résultat réel de la politique d'accès au module	Ce champ est fourni à titre d'information et est en lecture seule.
Module de chiffrement parent	Module cryptographique parent, qui est déterminé par le type de module cryptographique que vous avez sélectionné à l'étape précédente. Ce champ est en lecture seule.

4. Sélectionnez **Soumettre**.

Créer un groupe secret de base

Créez un groupe secret de base pour regrouper tous les secrets, quels que soient leurs critères.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Les groupes secrets de base peuvent contenir n'importe quel secret que vous leur ajoutez, quels que soient leur table, leur périmètre ou leur application. Après l'avoir créé, vous ajoutez manuellement des secrets au groupe. Pour créer un groupe spécifique à tous les secrets qui partagent un attribut commun, créez un groupe secret avec des critères en suivant les instructions de la section Créer un groupe secret avec des critères.

Procédure

1. Accédez à la **Tous** > **Gestion des secrets** > **Groupes secrets**.
2. Sélectionnez **Nouveau**.
3. Dans le **champ Quel type de groupe secret voulez-vous créer ?** sélectionnez **Groupe secret de base**.
4. Dans le formulaire **Groupe secret** , renseignez les champs.

Champs de groupes secrets

Champ	Description
Nom de groupe	Nom pour le groupe **Remarque :** Les noms de groupes secrets ne peuvent contenir que des minuscules, des chiffres et des traits de soulignement (_)
Type de secret	Indique si le groupe est **accessible à l'instance** ou **accessible au client**.
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et déchiffre vos données. Ce champ est activé par défaut.
Application	L'application incluse dans le périmètre pour cet enregistrement. Ce champ en lecture seule est automatiquement renseigné avec le champ d'application actuel.
Description brève	Description du groupe
Module de chiffrement	Sélectionnez le module cryptographique à utiliser avec ce groupe. Ce module crypte et déchiffre vos données. Ce champ n'est visible que lorsque Module de **génération automatique** n'est pas sélectionné. Pour plus de détails sur les politiques d'accès au module, voir Vue d'ensemble de la politique d'accès au module **Remarque :** Vous pouvez consulter les politiques d'accès au module associées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Envoyer**.

> **Remarque :**
> Lorsqu'il est créé, un groupe secret est inactif par défaut. Revenez à l'enregistrement du groupe et sélectionnez **Actif** pour activer le groupe.

Créer un groupe secret avec des critères

Créez un groupe secret avec des critères permettant d'organiser automatiquement les secrets saisis dans les champs Password2 lorsqu'ils partagent un critère commun, tel qu'une table, un périmètre ou une application.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

Les secrets au sein de ce type de groupe secret doivent tous partager des critères communs. Pour les groupes sans cette restriction, envisagez de créer un groupe secret de base. Découvrez comment créer un groupe secret de base dans Créer un groupe secret de base.

Procédure

1. Accédez à la **Tous** > **Gestion des secrets** > **Groupes secrets**.
2. Sélectionnez **Nouveau**.
3. Dans **le menu Quel type de groupe secret voulez-vous créer ?** , sélectionnez **Groupe secret avec critères**.
4. Dans le formulaire **Groupe secret** , renseignez les champs.

Champs de groupes secrets

Champ	Description
Nom de groupe	Nom pour le groupe **Remarque :** Les noms de groupes secrets ne peuvent contenir que des minuscules, des chiffres et des traits de soulignement (_)
Type de secret	Indique si le groupe est **accessible à l'instance** ou **accessible au client.**
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et déchiffre vos données. Ce champ est activé par défaut.
Application	L'application incluse dans le périmètre pour cet enregistrement. Ce champ en lecture seule est automatiquement renseigné avec le champ d'application actuel.
Description brève	Description du groupe
Type de critère	Critères partagés par les secrets de ce groupe. ○ Champ d'application ○ Package

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Table cible ○ Colonne secrète ○ Filtrer l'enregistrement
Module de chiffrement	Sélectionnez le module cryptographique à utiliser avec ce groupe. Ce module crypte et déchiffre vos données. Ce champ n'est visible que lorsque Module de **génération automatique** n'est pas sélectionné. Pour plus de détails sur les politiques d'accès au module, voir Vue d'ensemble de la politique d'accès au module **Remarque :** Vous pouvez consulter les politiques d'accès au module associées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

Remarque : Selon votre configuration, le **module de chiffrement** peut utiliser une valeur sélectionnée automatiquement.

Lorsque le champ **Type de critère** est défini sur Package et que le champ **Module de génération automatique** est sélectionné :	Le champ **Module de chiffrement** est vide et en lecture seule. Un sous-module Password2 existant est utilisé. Si aucun sous-module Password2 n'est trouvé, le module Glide Encrypter au niveau de l'instance est utilisé.
Lorsque le champ **Type de critère** est défini sur Package et que le champ Module de **génération automatique** est désélectionné : (le champ **Module de génération automatique** ne peut être désélectionné que par les utilisateurs Enterprise)	Le champ **Module de chiffrement** est modifiable et les administrateurs peuvent sélectionner un module de chiffrement à utiliser.

5. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Remarque : Lorsqu'il est créé, un groupe secret est inactif par défaut.

6. Après avoir sauvegardé l'enregistrement, des champs supplémentaires peuvent apparaître en fonction de la façon dont vous avez configuré votre groupe.

Champs supplémentaires de groupes secrets

Champ	Description
Périmètre cible	Périmètre partagé par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous

Traduction automatique

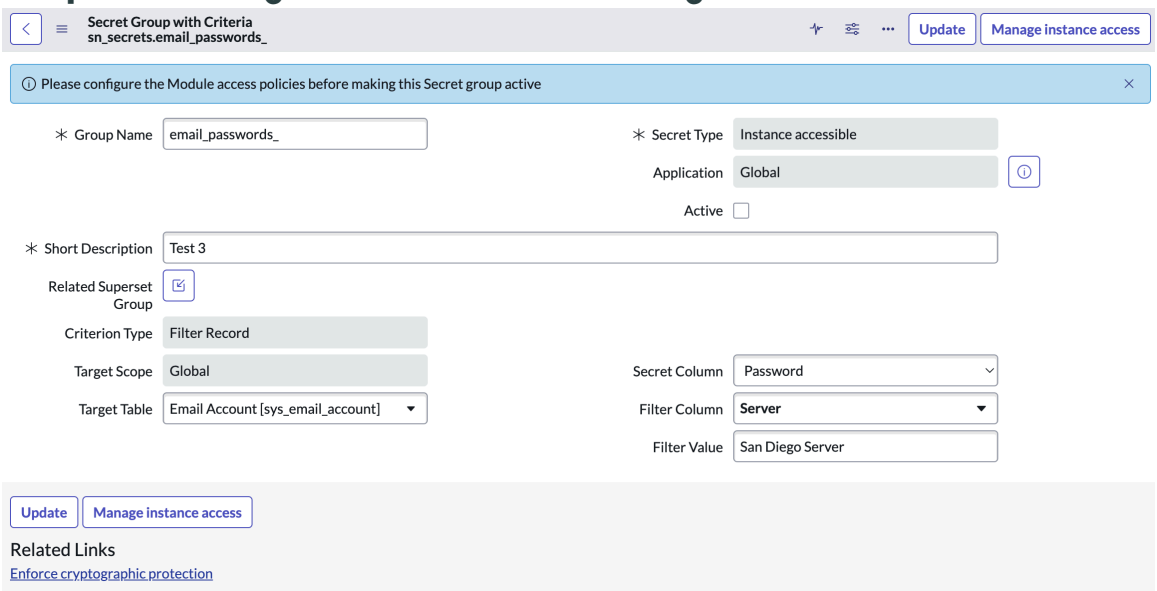
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	sélectionnez Périmètre dans le champ **Type de critère** .
Package cible	Package partagé par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous sélectionnez Package dans le champ **Type de critère** .
Table cible	Table partagée par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous sélectionnez Table ou Colonne secrète dans le champ **Type de critère** .
Périmètre cible	Périmètre de l'application de la table sélectionnée dans le champ **Table cible** . Ce champ est uniquement visible lorsque vous sélectionnez Table, Colonne de filtre ou Colonne secrète dans le champ **Type de critère** .
Colonne secrète	Colonne de table contenant les secrets pasword2 que vous incluez dans ce groupe. Les champs disponibles dans cette liste sont déterminés par la table sélectionnée dans le champ **Table cible** . **Remarque :** Si aucune colonne dans la table de sélection ne contient de secrets, ce champ affiche uniquement (Aucun) sous forme de sélection.
Colonne de filtre	La colonne de la table sélectionnée dans la **table cible** que vous souhaitez utiliser comme filtre. Ce champ ne peut pas être un champ Password2.
Valeur de filtre	La valeur que vous souhaitez utiliser comme filtre. Ce filtre s'applique à la sélection de champ dans le champ **Colonne de filtre** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Groupe accessible à l'instance contenant tous les mots de passe de compte de messagerie d'un serveur de messagerie



Que faire ensuite

Après la création de votre groupe, tous les nouveaux enregistrements correspondant aux critères seront chiffrés. Pour chiffrer des enregistrements existants à l'aide du module de chiffrement de ce groupe, vous devez exécuter une tâche de sécurité. Pour plus de détails, voir Exécuter les tâches de sécurité de gestion des secrets.

Les groupes accessibles aux clients ont besoin d'une clé publique fournie par le client pour chiffrer vos secrets. Pour connaître la procédure de chargement de cette clé, reportez-vous à la section Charger une clé publique pour la gestion des secrets.

Charger une clé publique pour la gestion des secrets

Téléchargez une clé publique pour chiffrer vos secrets.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Gestion des secrets** > **Groupes secrets**et ouvrez l'enregistrement de groupe secret.
2. Dans l'enregistrement, sélectionnez le bouton **Gérer l'accès côté client** .
   Un nouvel enregistrement de groupe d'identités s'ouvre.
3. Sélectionnez le bouton **Télécharger la clé d'identité** .
   Une fenêtre **Certificat de clé publique d'identité d'importation** s'affiche.
4. Entrez un alias pour votre clé dans le champ **Alias de clé d'identité** .
5. Sélectionnez le bouton **Importer** pour télécharger la clé à partir de votre environnement local.
6. Sélectionnez le bouton **OK** .
   Le champ **Clé du module de groupe** utilise le nom d'alias de la clé d'identité.
7. Sélectionnez **Soumettre** pour sauvegarder l'enregistrement du groupe d'identités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter les tâches de sécurité de gestion des secrets

Planifiez une tâche de gestion des secrets pour effectuer des tâches de chiffrement sur les champs secrets de votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin, security_admin et sn_secrets.admin

Pour effectuer ces étapes, vous devez accéder au rôle security_admin. Pour plus de détails sur ce processus, voir Élever à un rôle privilégié

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de gestion des secrets**.
3. Remplissez les champs du formulaire.

Formulaire de tâche de gestion des secrets

Champ	Description
Nom	Nom de la tâche de sécurité
État	L'état initial de la tâche est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état est mis à jour en conséquence
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures. L'exécution de la tâche commence à l'heure choisie.
Fin de la fenêtre de temps	Heure de fin de la tâche au format 24 heures. Si la tâche n'est pas terminée à ce moment-là, elle se poursuit pendant la fenêtre de traitement spécifiée suivante jusqu'à ce que la tâche soit terminée.
Niveau de mise en application	Indique si la tâche affecte toutes les tables, ou une sélection de tables ou de champs spécifiques. Sélectionnez parmi ○ Toutes les tables ○ Tables spécifiques ○ Champs spécifiques ○ Packages spécifiques **⚠ Avertissement :** La sélection de l'option **Toutes les tables** peut affecter les performances de l'instance. Envisagez une planification en dehors des heures de pointe.
Packages	Packages à inclure dans cette tâche. Le chiffrement est appliqué aux packages sélectionnés. Cette option s'affiche uniquement lorsque le champ **Niveau d'application** est défini sur **Packages spécifiques**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tables	Tables à inclure dans cette tâche. Le chiffrement est appliqué à tous les champs applicables dans les tables sélectionnées. Cette option s'affiche uniquement lorsque le **niveau d'application** est défini sur **Tables spécifiques**
Champs	Tables à inclure dans cette tâche. Le chiffrement est appliqué à tous les champs sélectionnés. Cette option s'affiche uniquement lorsque le **niveau de mise en application** est défini sur **Champs spécifiques**
Mode de tâche	Sélectionnez parmi **Password2 vers Gestion des secrets** Chiffrez tous les champs password2 dans vos secrets Les groupes utilisant les modules de chiffrement ont défini la politique d'accès au module de chaque groupe. **Gestion des secrets vers Password2** Chiffrez à nouveau les données dans vos groupes secrets à l'aide du chiffrement password2. Pour plus d'informations sur ce type de chiffrement, consultez Chiffrement Password2 avec KMF. **Mise en application d'un groupe secret** Interroge toutes les données qui doivent correspondre au groupe sélectionné dans le champ **Groupe secret** . Si toutes les données trouvées par la requête se trouvent déjà dans le groupe, la tâche n'apporte aucune modification. Si la requête trouve des données qui ne sont pas encore dans le groupe, la tâche chiffre à nouveau ces données au sein du groupe secret. **Remarque :** Si les données trouvées dans cette requête sont déjà chiffrées et que vos instances ne peuvent pas déchiffrer ces données, elles ne sont pas chiffrées et ajoutées au groupe secrets.
Groupe secret	Groupe secret contenant les secrets à chiffrer. Ce champ n'est disponible que lorsque **Groupe secret** est sélectionné dans le champ **Mode de tâche** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Forcer la nouvelle saisie des données	
Résumé	Affiche des informations sur la progression de la tâche. Le résumé affiche également les enregistrements qui n'ont pas pu être chiffrés par la tâche.

4. Sélectionnez **Soumettre**.

Que faire ensuite

La tâche interroge toutes les données qui doivent correspondre au groupe secret sélectionné. Si toutes les données trouvées par la requête se trouvent déjà dans le groupe, la tâche n'apporte aucune modification. Si la requête trouve des données qui ne sont pas encore dans le groupe, la tâche chiffre à nouveau ces données au sein du groupe secret. (Si l'instance peut le déchiffrer, ce qui peut ne pas être le cas pour les secrets chiffrés côté client).

Signature de code

La signature de code crée des signatures numériques pour les données, qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. La signature de code est un module sous licence en tant que composant de ServiceNow Coffre-fort.

Signature de code et cercle de confiance

Le Cercle de confiance (COT) est un prérequis pour la signature de code qui crée une communication sécurisée entre vos instances approuvées et protégées afin de garantir que seuls les utilisateurs autorisés peuvent accéder à la fonctionnalité de signature de code.

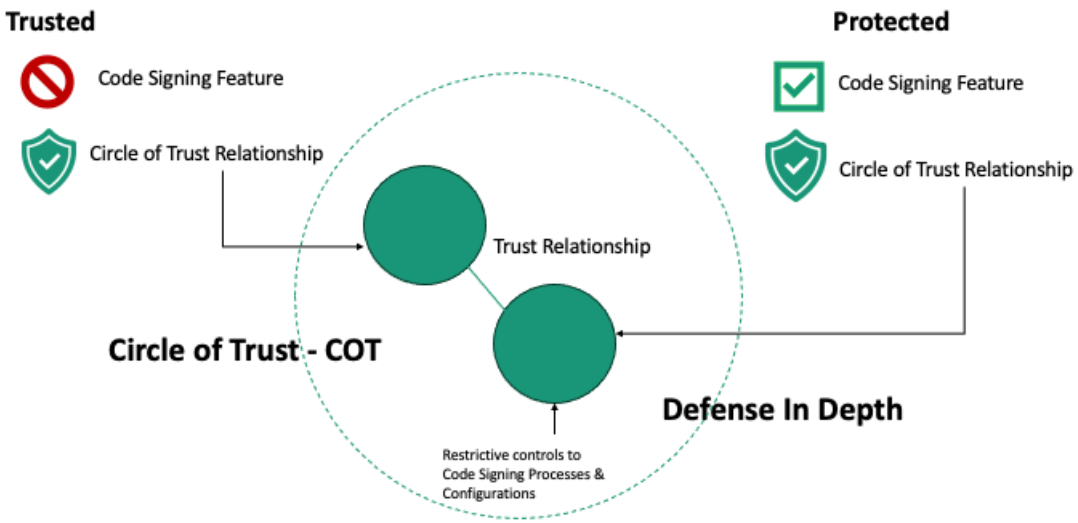
Plusieurs mesures de sécurité permettent d'empêcher les acteurs malveillants de désactiver ou d'utiliser à mauvais escient la signature de code en cas de compromission d'une instance protégée. Dans le cadre de la stratégie de défense en profondeur, l'utilise COT les éléments suivants :

- Les contrôles qui restreignent même les comptes administrateur les plus puissants sont établis dans l'instance protégée pour aider à protéger les processus et la configuration de Code Signing.
- Les instances approuvées doivent collaborer avec les instances protégées pour établir la Cercle de confiance relation. Au moins une instance approuvée est requise, mais plusieurs instances approuvées peuvent être configurées pour collaborer avec l'instance protégée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du cercle de confiance

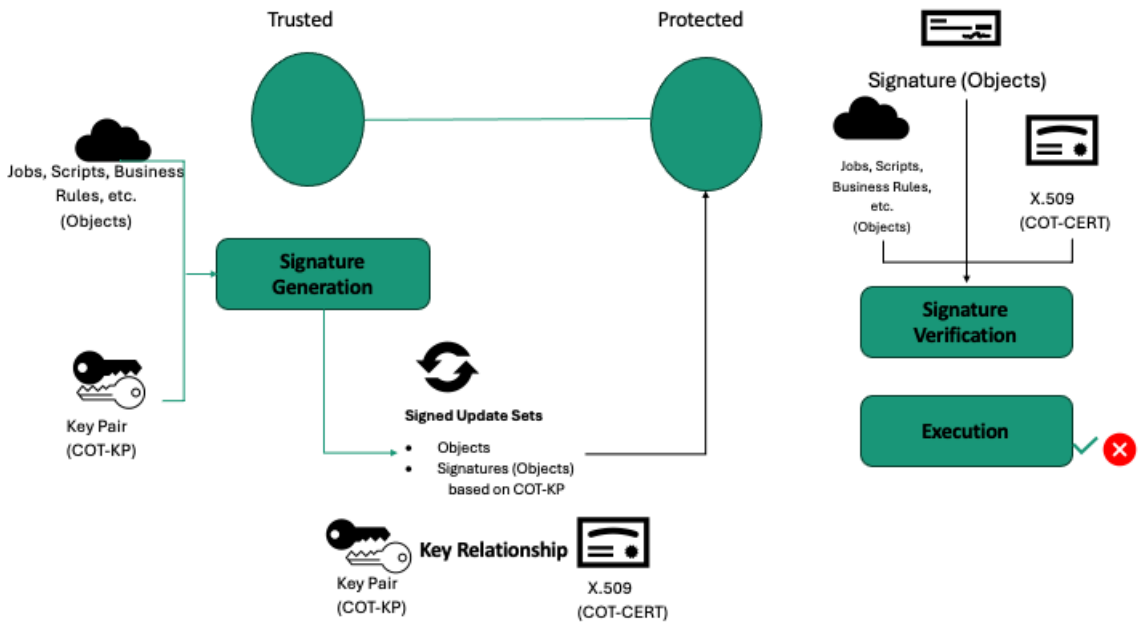


L'utilise Cercle de confiance des tâches, des scripts et des règles métier ainsi qu'une paire de clés pour générer des signatures afin de signer des ensembles de mises à jour sur l'instance protégée. Lorsque la tâche est appelée, la signature est vérifiée ainsi que le certificat approuvé pour exécuter les mises à jour d'instance protégées.

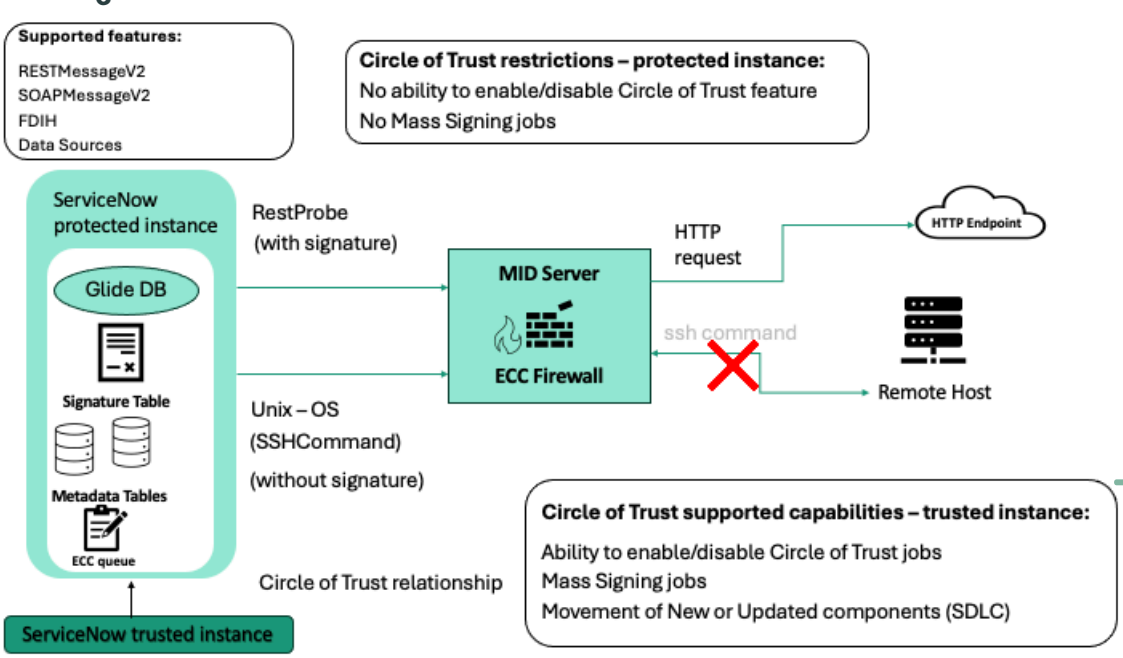
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Processus d'ensembles de mises à jour approuvés



Flux de signature de code



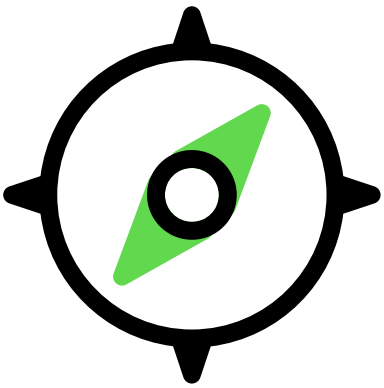
Traduction automatique

Cela Cercle de confiance nécessite une relation de confiance initiale entre les instances approuvées et protégées qui empêche tout utilisateur non autorisé disposant de n'importe quel niveau d'autorisation d'accéder à des activités non approuvées.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

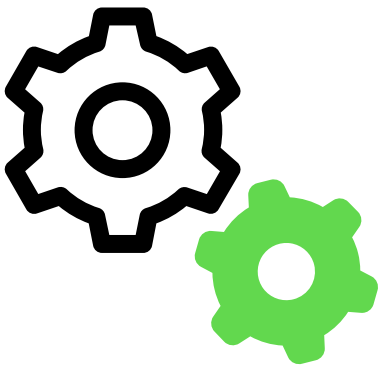
Premiers pas

Explorer



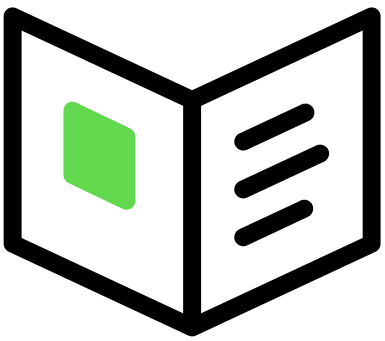
Découvrez les principales fonctionnalités et la valeur commerciale de la signature de code.

Configurer



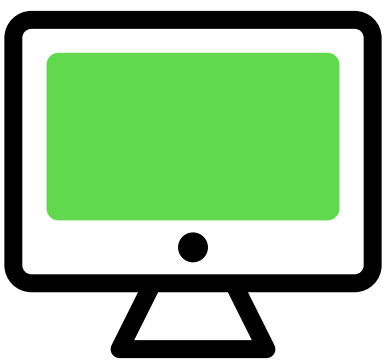
Activez et configurez la signature de code.

Référence



Obtenir des détails sur les propriétés et le dépannage

Utiliser



Découvrez comment utiliser la signature de code pour vérifier l'authenticité et l'intégrité de vos données.

Dépannage et demande d'aide

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer la signature de code

La signature de code fournit une vérification cryptographique pour s'assurer que seuls les scripts autorisés peuvent s'exécuter sur les serveurs MID. La signature de code empêche le traitement des enregistrements de file d'attente ECC non autorisés ou falsifiés par les MID Server, préservant ainsi l'intégrité des intégrations entre ServiceNow et les systèmes externes.

La signature de code crée des signatures numériques pour vos données, qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. La signature de code est un module sous licence en tant que composant de ServiceNow Coffre-fort.

Remarque :
L'équipe Service client et assistance doit accorder l'accès à la signature de code.

La signature de code déclare l'intention derrière l'opération en cours d'exécution et valide si la ressource ou l'enregistrement peut être utilisé aux fins prévues. Pour faciliter la signature de code, le (KMF) utilise des certificats numériques et un Cadre de travail de gestion des clés chiffrement asymétrique standard pour les signatures numériques.

Utilisez la signature de code en interne côté plateforme et infrastructure. La signature de code permet de signer le contenu de tables spécifiques ou d'un sous-ensemble d'enregistrements dans une table de métadonnées donnée.



La signature de code utilise un () sécurisé Cercle de confiance entreCOT vos instances approuvées et protégées pour garantir que seules les instances approuvées autorisées et sécurisées peuvent accéder à la fonctionnalité de signature de code.

Remarque :
La signature de code est activée sur l'instance protégée et non sur l'instance approuvée.

Comment la signature de code protège votre environnement

Sans signature de code, un attaquant qui accède aux ServiceNow enregistrements peut modifier les instructions SQL dans une instance protégée. Lorsque le Serveur MID traite cette demande de source de données, il exécute les commandes SQL malveillantes, ce qui peut compromettre l'intégrité et la sécurité du système.

Lorsque vous implémentez une architecture de cercle de confiance avec signature de code, le transfert des données vers le serveur MID suit le processus de vérification suivant. Ce processus permet de s'assurer que seul le code autorisé provenant de l'instance approuvée peut s'exécuter sur le serveur MID. Les processus réduisent les vecteurs d'attaque potentiels qui pourraient autrement compromettre vos systèmes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Les signatures numériques sont appliquées aux sources de données créées ou mises à jour au sein de l'instance approuvée.
2. Utilisez le processus de signature de code pour transférer les données signées de l'instance approuvée vers l'instance protégée
3. Le Serveur MID vérifie la signature numérique sur toutes les demandes entrantes, rejetant automatiquement toutes les demandes pour lesquelles il n'y a pas de signature valide.
4. Si le serveur MID rejette une demande, il consigne ce rejet et envoie une notification à l'instance protégée.

Avantages de la mise en œuvre de la signature de code

La signature de code offre plusieurs avantages clés :

Contrôle d'exécution

Seuls les scripts vérifiés par cryptographie peuvent s'exécuter sur les serveurs MID

Détection d'altération

Toute modification apportée aux enregistrements signés est immédiatement identifiée et bloquée.

Protection automatisée

Le système gère l'application de la sécurité sans nécessiter d'intervention manuelle.

Journalisation complète

Tous les échecs de vérification de signature génèrent des enregistrements d'audit détaillés.

Validation de la signature de code et tâches

Toutes les tables de métadonnées avec des configurations valides sont signées au moment de la création à l'aide du module d'extension de métadonnées de signature de code (`com.glide.code_signing`). Si vous choisissez de signer les tables, les utilisateurs administrateurs disposant du rôle d'administrateur de sécurité ont accès aux tâches de chiffrement de signature de code :

- Signer les ensembles de mises à jour.
- Signer en masse des enregistrements.
- Signer en masse des pièces jointes.

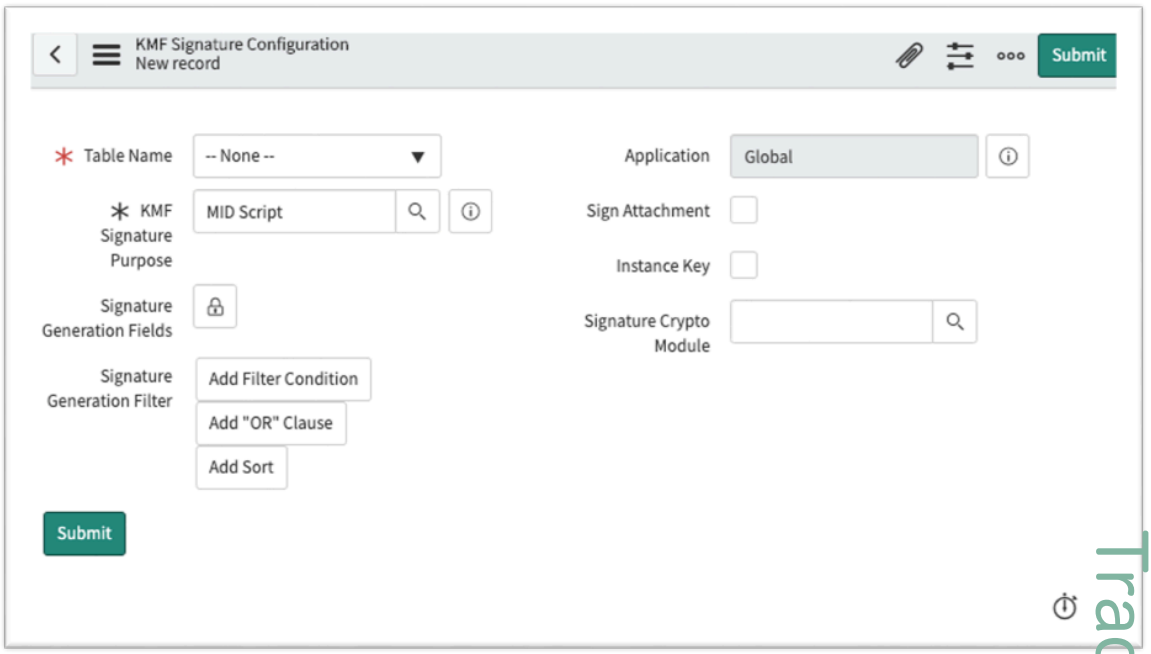
Signer l'ensemble de mises à jour

Cette tâche signe les enregistrements qui correspondent à une configuration de signature dans l'ensemble de mises à jour. La tâche ajoute également tous les nouveaux enregistrements de signatures et les certificats de vérification à l'ensemble de mises à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement de signature KMF pour l'ensemble de mises à jour



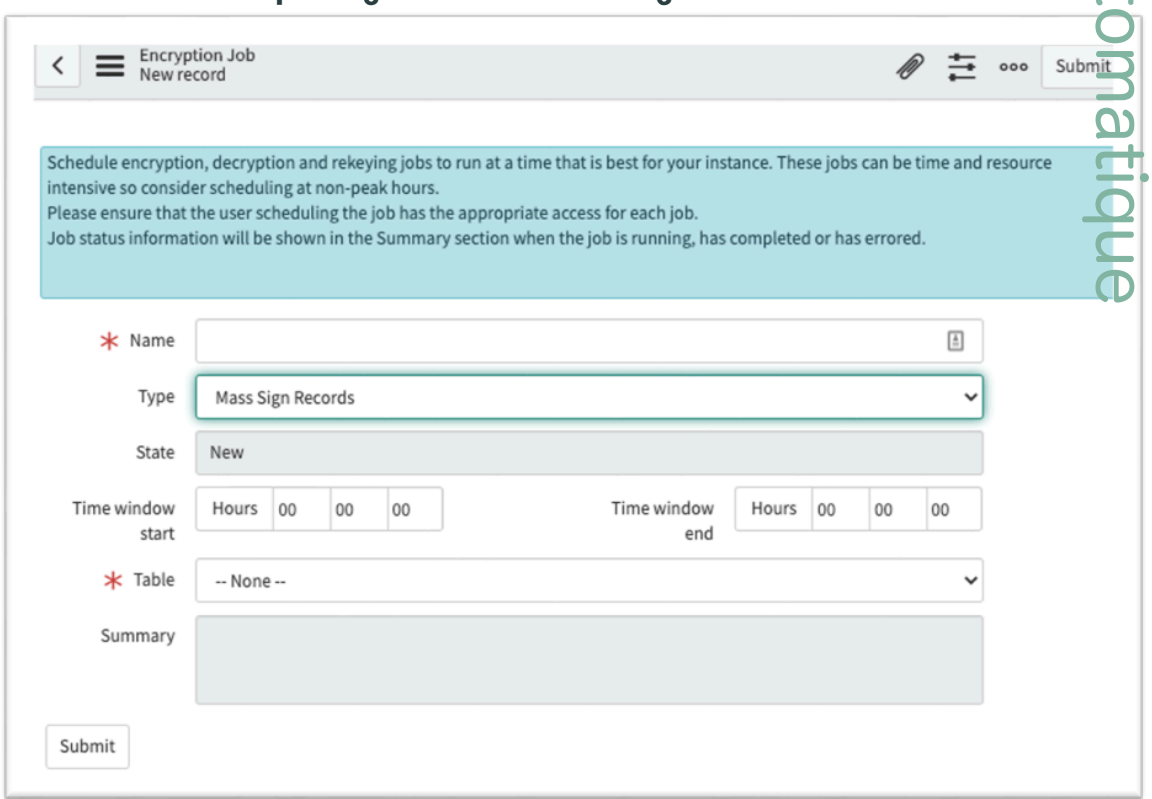
Signer en masse les enregistrements

Cette tâche signe tous les enregistrements qui correspondent à la configuration de signature appliquée sur une table de métadonnées spécifique.

Signer en masse les pièces jointes

Cette tâche signe tous les enregistrements de pièce jointe joints à une table qui correspond à une configuration de signature spécifiée.

Tâche de chiffrement pour signer en masse les enregistrements

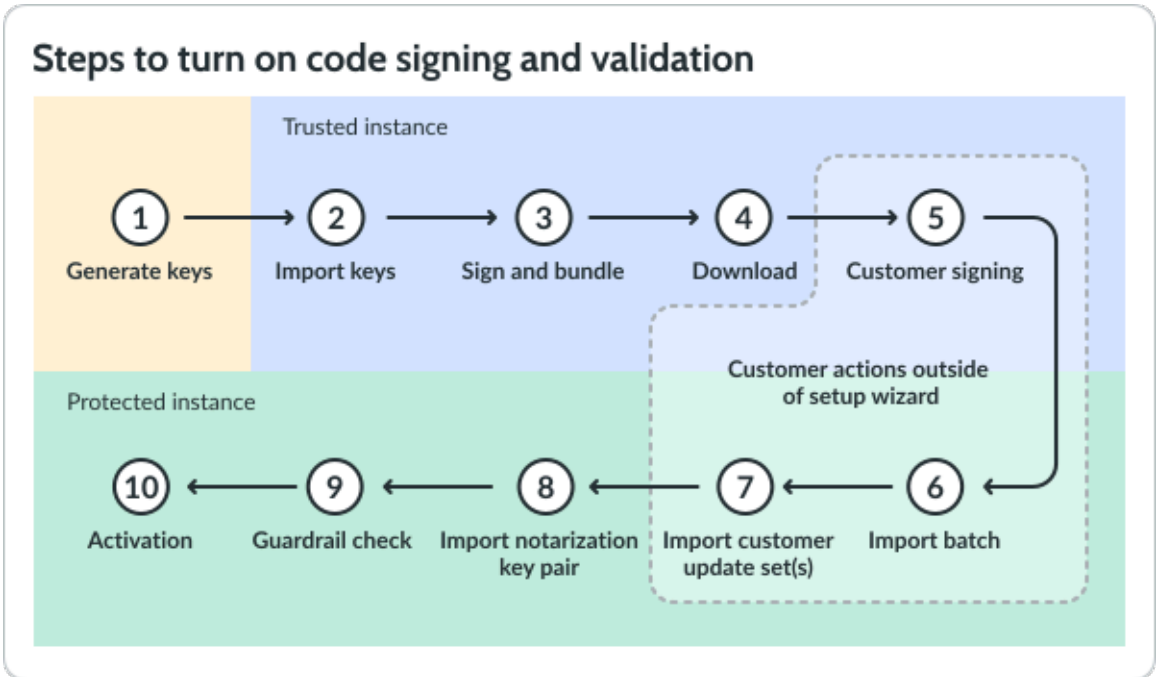


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la signature de code

Activez et configurez la signature de code pour vérifier l'authenticité et l'intégrité de vos données.



Code Signing Enterprise nécessite une relation de confiance initiale entre des instances approuvées et protégées qui permet d'empêcher tout utilisateur non autorisé, quel que soit le niveau d'autorisation, d'accéder à des activités non approuvées.

Reportez-vous à chaque rubrique pour compléter les étapes de configuration afin d'établir le Cercle de confiance avec Code Signing Enterprise :

Affecter le rôle d'administrateur de signature de code

Affectez le rôle d'administrateur de signature de code à un utilisateur pour accéder à l'expérience de configuration de la signature de code.

Configurez Code Signing Enterprise sur votre instance de confiance

Activez la signature de code sur votre instance de confiance.

Chargez votre fichier de configuration de signature de code sur votre instance protégée

Chargez le fichier de configuration généré sur votre instance de confiance.

Configurez Code Signing Enterprise sur votre instance protégée

Activez et configurez la signature de code sur votre instance protégée.

Activer la validation de certificat

Activez la validation de certificat sur votre instance.

Désactiver la signature de code

Désactivez la signature de code sur votre instance protégée.

Remarque :
Cette étape facultative ne fait pas partie de la configuration initiale de la signature de code

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecter le rôle d'administrateur de signature de code

Affectez le rôle d'administrateur de signature de code à un utilisateur pour accéder à l'expérience de configuration de la signature de code.

Avant de commencer

Rôles requis :

- administrateur
- security_admin

Important :
L'utilisateur auquel le rôle d'administrateur de signature de code est affecté doit se trouver dans le champ d'application global.

Procédure

1. Sélectionnez une instance de confiance à utiliser.
   L'instance approuvée est utilisée pour créer des tâches, signer des enregistrements et effectuer d'autres tâches nécessaires avant d'activer la validation de signature sur votre instance protégée.
2. Accédez à la **Tous** > **Signature de code** > **Administration** > **Administration du rôle**.
3. Accordez à un utilisateur le rôle d'administrateur de signature de code en déplaçant un utilisateur de la liste des **utilisateurs disponibles** vers la liste **des utilisateurs sélectionnés** .
4. Sélectionnez **Enregistrer**.

Important :
L'utilisateur affecté au rôle doit se déconnecter et se regrouper à nouveau pour effectuer des tâches de signature de code.

Résultats

L'utilisateur sélectionné a le rôle d'administrateur de signature de code. Un utilisateur disposant de ce rôle peut accéder à l'expérience de configuration de la signature de code et affecter d'autres rôles de signature de code aux utilisateurs.

Pour en savoir plus sur les rôles de signature de code, reportez-vous à la section Rôles installés avec Signature de code.

Configurez Code Signing Enterprise sur votre instance de confiance

Activez et configurez la signature de code sur votre instance de confiance.

Avant de commencer

Rôles requis :

- administrateur
- security_admin
- codesigning_admin

Remarque :
Le rôle codesigning_admin peut être affecté à l'aide du processus détaillé à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez disposer d'au moins une paire de clés cryptographiques et d'un certificat (extension de fichier p12) pour la signature client et l'administration du cercle de confiance (COT). Pour améliorer la sécurité, envisagez d'utiliser des paires de clés cryptographiques distinctes pour la signature client et l'administration COT.

Avertissement :
Une fois ce processus terminé, vous aurez téléchargé un fichier de configuration qui doit être installé sur votre instance protégée dans l'heure. Vérifiez que vous disposez du temps après ce processus pour charger le fichier de configuration sur votre instance protégée. Pour obtenir plus de détails sur ce processus, voir Chargez votre fichier de configuration de signature de code sur votre instance protégée.

Procédure

1. Sur votre instance de confiance, accédez à **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** pour ouvrir la page de configuration de signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **l'instance de confiance**.
3. Sélectionnez le bouton **Suivant** .
4. Dans le champ **Action** , sous **Sélectionner l'action que vous souhaitez accomplir**, sélectionnez **Activer la signature de code**.
5. En regard **de Pièces jointes** , dans la section **Paire de clés de signature du client et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.

   Conseil :
   Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre global et que vous disposez du rôle sn_kmf.cryptographic_manager.

6. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
7. Sélectionnez **Importer**.
8. Sélectionnez **Continuer** pour passer à la section suivante.
9. En regard **de Pièces jointes** , dans la section **Paire de clés et certificat d'administration COT** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.
10. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
11. Sélectionnez **Importer**.
12. Sélectionnez **Continuer** pour passer à la section suivante.
13. Sur la page Exporter le fichier **de configuration** , sélectionnez **Exporter** pour créer et télécharger un fichier de configuration utilisé pour activer la signature de code sur votre instance protégée.
    Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes détaillées dans Configurez Code Signing Enterprise sur votre instance protégée.

    Remarque :
    La signature de code applique des limites sur les ensembles de mises à jour volumineux afin d'améliorer l'expérience utilisateur. La taille maximale d'un ensemble de mises à jour est de 10 000 enregistrements.

Chargez votre fichier de configuration de signature de code sur votre instance protégée

Chargez le fichier de configuration généré sur votre instance de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôles requis :

- administrateur
- security_admin
- codesigning_admin

Remarque :
Le rôle codesigning_admin peut être affecté à l'aide du processus détaillé à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Vous avez également besoin du fichier de configuration généré lors des étapes détaillées dans .Configurez Code Signing Enterprise sur votre instance de confiance

Procédure

1. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
2. Sélectionnez **Importer un ensemble de mises à jour à partir d'un fichier XML** en bas de la liste **Ensembles de mises à jour récupérés** .
3. Sélectionnez **Choisir un fichier**, puis sélectionnez votre fichier de configuration (extension de fichier XML).
4. Sélectionnez **Charger**.
   Vous devez voir l'ensemble de mises à jour de **configuration de signature** dans la liste **Ensembles de mises à jour récupérés** .
5. Sélectionnez et ouvrez l'ensemble de mises à jour **de la configuration de signature de caractères** .
6. Sélectionnez **Aperçu du lot d'ensembles de mises à jour**.
   Si des conflits se produisent pendant l'aperçu, résolvez-les en sélectionnant **Accepter la mise à jour distante** ou **Résoudre les conflits CS connus**.
7. Après avoir résolu les conflits, sélectionnez **Valider le lot d'ensemble de mises à jour**.

Configurez Code Signing Enterprise sur votre instance protégée

Activez et configurez la signature de code sur votre instance protégée.

Avant de commencer

Rôles requis :

- administrateur
- security_admin
- codesigning_admin

Remarque :
Le rôle codesigning_admin peut être affecté à l'aide du processus détaillé à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur votre PPI, accédez à **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** pour ouvrir la page de configuration de signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **Instance protégée**.
3. Sélectionnez le bouton **Suivant** .
4. Cochez la case **Veuillez confirmer que l'ensemble de mises à jour de configuration de signature de code a été importé et validé** .
5. Sélectionnez le bouton **Suivant** .
6. Attendez la fin de l'installation du certificat.
   Un message d'alerte bleu s'affiche et indique que les éléments du fichier de configuration sont en cours d'installation. L'alerte disparaît au bout de quelques secondes à la fin de l'installation.
7. En regard **de Pièces jointes** , dans la section **Paire de clés d'exécution/de notarisation et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser à des fins d'exécution/de notarisation.
   Vous pouvez réutiliser une paire de clés de l'instance approuvée ou en charger une nouvelle spécifiquement pour cette utilisation.

   Conseil :
   Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre global et que vous disposez du rôle sn_kmf.cryptographic_manager.

8. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
9. Sélectionnez **Importer**.
10. Sélectionnez **Continuer** pour passer à la section suivante.
11. Attendez que votre instance effectue une vérification des garde-fous.
    Cette vérification analyse votre instance à la recherche de signatures non valides et peut prendre un certain temps. Ne quittez pas ou n'actualisez pas la page tant que l'analyse n'est pas terminée.

    Ce workflow identifie les signatures qui ont été générées avec des certificats expirés ou inactifs et signe à nouveau les enregistrements concernés. Pour améliorer les performances, le workflow divise maintenant le processus en plusieurs événements et les exécute en parallèle.

12. Si l'analyse trouve des signatures non valides, sélectionnez **Télécharger le rapport**.

    La sélection **de Télécharger le rapport** télécharge un rapport (scan_report.txt) que vous pouvez utiliser pour examiner et corriger les signatures non valides.

    Après avoir résolu les erreurs, actualisez la page pour réexécuter la vérification.

13. S'il n'y a pas d'erreur, sélectionnez **Terminer la configuration**.
14. Attendez que les tâches de configuration soient terminées.
    Votre instance exécute une ou plusieurs tâches pour terminer le processus de configuration. Ne quittez pas la page et ne l'actualisez pas tant que les tâches ne sont pas terminées. Lorsque vous avez terminé, vous devez voir un message **de configuration de signature de code terminée avec succès** .

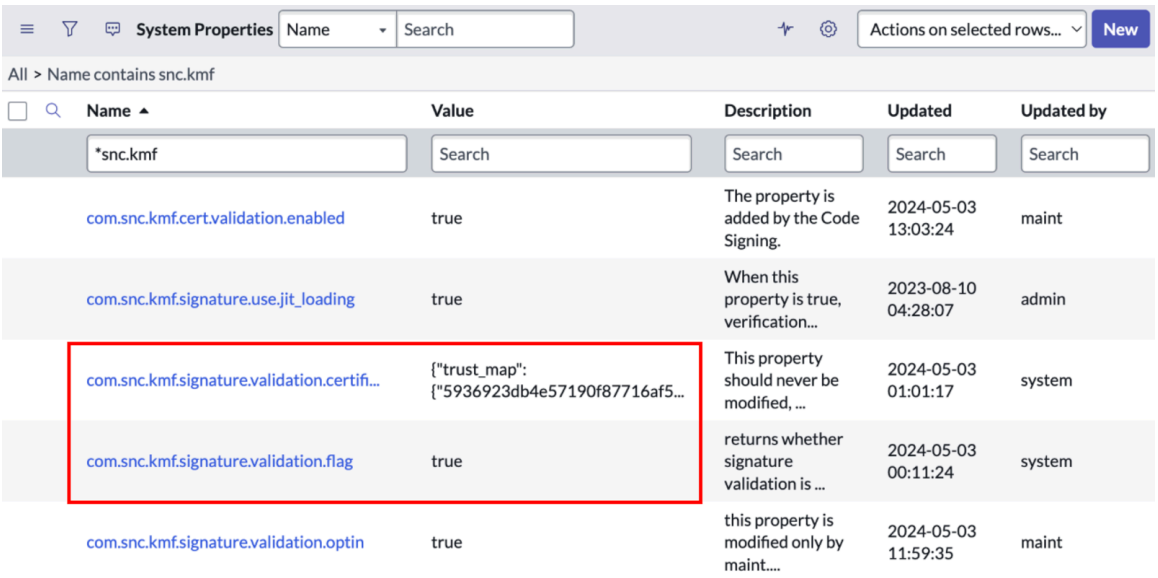
Résultats

La validation de la signature est maintenant appliquée sur votre instance de production. Vous pouvez vérifier la réussite de l'exécution en consultant les propriétés de votre système. Recherchez la propriété **com.snc.kmf.signature.validation.flag** dans la table

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système [sys_property] et vérifiez que sa valeur est **true**. Vérifiez que la propriété **com.snc.kmf.signature.validation.certificate_trust** n'a pas une valeur vide.



Name	Value	Description	Updated	Updated by
*snc.kmf	Search	Search	Search	Search
com.snc.kmf.cert.validation.enabled	true	The property is added by the Code Signing.	2024-05-03 13:03:24	maint
com.snc.kmf.signature.use.jit_loading	true	When this property is true, verification...	2023-08-10 04:28:07	admin
com.snc.kmf.signature.validation.certifi...	{"trust_map": {"5936923db4e57190f87716af5...	This property should never be modified, ...	2024-05-03 01:01:17	system
com.snc.kmf.signature.validation.flag	true	returns whether signature validation is ...	2024-05-03 00:11:24	system
com.snc.kmf.signature.validation.optin	true	this property is modified only by maint....	2024-05-03 11:59:35	maint

Activer la validation de certificat

Protégez votre instance avec une validation basée sur un certificat.

Avant de commencer

Rôle requis :

- codesigning_admin
- security_admin
- sn_kmf.cryptographic_manager

Procédure

1. Sur votre instance de confiance, accédez à **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** pour ouvrir la page de configuration de signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **l'instance de confiance**.
3. Sélectionnez le bouton **Suivant** .
4. Dans le champ **Action** , sous **Sélectionnez l'action que vous souhaitez accomplir**, sélectionnez **Activer la validation de certificat**.
5. Sélectionnez le bouton **Suivant** .
6. En regard **de Pièces jointes** , dans la section **Paire de clés de signature du client et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.

   Conseil :
   Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre global et que vous disposez du rôle sn_kmf.cryptographic_manager.

7. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
8. Sélectionnez **Importer**.
9. Sélectionnez **Continuer** pour passer à la section suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. En regard **de Pièces jointes** , dans la section **Paire de clés et certificat d'administration COT** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.
11. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
12. Sélectionnez **Importer**.
13. Sélectionnez **Continuer** pour passer à la section suivante.
14. Dans la section **Effectuer des tâches d'instances de confiance** , attendez que toutes les tâches soient terminées.

    Votre instance génère et exécute automatiquement ces tâches. Si vous avez utilisé la signature de code avant la mise en production, des Vancouver tâches sont créées et exécutées pour mettre à jour vos signatures.

    Dans certains cas, aucune tâche n'est nécessaire. **Aucune tâche nécessaire ne** s'affiche sur cette page.
15. Sélectionnez **Continuer** pour passer à la section suivante.
16. Sur la page Exporter le fichier **de configuration** , sélectionnez **Exporter** pour créer et télécharger un fichier de configuration utilisé pour activer la signature de code sur votre instance protégée.
    Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes détaillées à la section Configurez Code Signing Enterprise sur votre instance protégée.
17. Sur votre instance protégée, accédez à **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
18. Sélectionnez **Importer un ensemble de mises à jour à partir d'un fichier XML** en bas de la liste **Ensembles de mises à jour récupérés** .
19. Sélectionnez **Choisir un fichier**, puis sélectionnez votre fichier de configuration (extension de fichier XML).
20. Sélectionnez **Charger**.
21. Revenir à la page de configuration de la signature de code à l'adresse **Tous** > **Signature de code** > **Configuration de la signature de code**.
22. Utilisez l'assistant pour terminer votre configuration, en sélectionnant les options pour terminer l'activation de la validation du certificat.

Révocation de certificat contrôlée par quorum

La révocation Signature de code des certificats contrôlée par le quorum fournit un mécanisme sécurisé permettant à un Signature de code administrateur de révoquer Signature de code les certificats. Le processus de révocation implique l'envoi d'une demande qui nécessite l'approbation de plusieurs personnes concernées. Ce workflow permet d'éviter les révocations accidentelles ou non autorisées.

Cette rubrique fournit une vue d'ensemble du processus de haut niveau pour la révocation sécurisée des certificats entre une instance de confiance et une instance protégée à l'aide d'un workflow d'approbation basé sur le quorum.

- Création et exportation de demandes (instance de confiance) : Initiez une révocation de certificat de quorum en créant une demande avec les propriétés de configuration requises. Exportez l'ensemble de mises à jour, qui inclut la demande de révocation et les données connexes. Reportez-vous à la rubrique Configuration de la demande de révocation de l'exportation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Importation et approbation (instance protégée) : importez l'ensemble de mises à jour dans l'instance protégée. Les approbateurs reçoivent des notifications et doivent terminer le workflow d'approbation avant que le certificat ne soit supprimé. Reportez-vous à la rubrique Importer la configuration de la demande de révocation.
- Redémarrage du serveur MID facultatif : si cette option est activée dans la configuration, les serveurs MID sur l'instance protégée sont redémarrés après la révocation du certificat. Cela force la resynchronisation immédiate du certificat, mais peut entraîner une perte de données pour les événements non traités ou mis en cache. Reportez-vous à la rubrique Approuver la révocation du certificat.

Remarque :

Ur *update set*expire après la fenêtre de temps définie par la propriété com.snc.kmf.signature.validity_window . S'il expire, vous pouvez exporter un nouvel ensemble de mises à jour signé à partir de l'instance approuvée. Cette fenêtre de validité s'applique à toutes les opérations de l'ensemble de mises à jour, y compris l'exportation, l'importation et l'activation Signature de code. Cette fenêtre de validité n'est pas liée à la fenêtre de temps de la demande que vous spécifiez lors de la création de la demande.

Configuration de la demande de révocation de l'exportation

Démarrez le processus de révocation du certificat en sélectionnant le certificat que vous souhaitez révoquer. Fournissez les propriétés de configuration requises. Exportez cette transaction dans le cadre d'un ensemble de mises à jour, qui est importé dans l'instance protégée pour approbation et exécution.

Avant de commencer

Rôle requis : sn_cse.codesigning_admin, sn_cse.quorum_requester, security_admin

Procédure

1. Sur votre instance de confiance, accédez à **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** et ouvrez la page de Signature de code configuration.
2. Dans le champ **Type d'instance** , sélectionnez **l'instance de confiance**.
3. Sélectionnez le bouton **Suivant** .
4. Dans le champ **Action** , sous **Sélectionner l'action que vous souhaitez accomplir**, sélectionnez **Révocation du certificat**.
   La page Demande de révocation de certification s'affiche.
5. Dans la page Sélectionner le certificat à révoquer, sélectionnez le certificat que vous souhaitez révoquer et sélectionnez **Initier la révocation**.
6. Configurez les exigences d'approbation pour la révocation de la certification.

   a. Dans le menu Exigences du quorum, saisissez les informations appropriées dans les champs de texte.

Propriétés des exigences de quorum

Propriété	Description
Nombre minimal d'approbations	Nombre minimal d'approbateurs requis pour approuver la demande de révocation de certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Intervalle de temps	Délai d'expiration de la demande de révocation.
Approbateurs	Adresse e-mail des utilisateurs autorisés à approuver la demande de révocation.

b. Dans le champ Description de la **demande** , saisissez le motif de révocation du certificat.

c. Sélectionnez **Enregistrer**.
Le menu Exporter le fichier de configuration s'affiche.

d. Sur la page Exporter le fichier de configuration, sélectionnez **Exporter** pour créer et télécharger un fichier de configuration utilisé pour exécuter le workflow de révocation de certificat sur votre instance protégée.

Résultats
Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes détaillées à la section Configurez Code Signing Enterprise sur votre instance protégée.

Importer la configuration de la demande de révocation

Importez l'ensemble de mises à jour dans l'instance protégée pour lancer le processus de révocation du certificat. Les approbateurs reçoivent des notifications par e-mail et doivent terminer le workflow d'approbation avant que le certificat ne soit révoqué. L'approbation signifie que les révocations sont confirmées, autorisées et traçables à des fins de sécurité et de conformité.

Avant de commencer
Rôle requis : sn_cse.codesigning_admin, sn_cse.quorum_requester, security_admin

Procédure

1. Connectez-vous à votre instance protégée et accédez à **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés** > **Importer XML**.
   La page Importer XML s'affiche.
2. Sélectionnez **Choisir un fichier** et sélectionnez le fichier XML de configuration dans votre système local.
3. Sélectionnez **Charger**.
4. Revenir à la page de configuration de la signature de code à l'adresse **Tous** > **Signature de code** > **Configuration de la signature de code**.

   a. Examinez les fichiers de configuration suivants dans l'onglet **Mises à jour du client par lots** .
   - Propriété de la configuration de la signature de code (`time_window`)
   - Propriété de configuration de la signature de code (`approver_email_ids`)
   - Propriété de configuration de la signature de code (`minimum_approvals`)
   - Propriété(`restart_mid_servers`) de configuration de la signature de code
   - Demande de quorum de signature de code (`CSEQCxxxxxxx`)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Transaction de signature de code (CSETRANSxxxxxxx)
- Enregistrements de signatures KMF

b. Sélectionner **Aperçu de l'ensemble de mises à jour par lots** > **Valider le lot d'ensemble de mises à jour**.

5. Revenir à la page de configuration de la signature de code à l'adresse **Tous** > **Signature de code** > **Configuration** > **Configuration guidée**.
6. Dans le champ **Type d'instance** , sélectionnez **Instance protégée** , puis **Suivant**.
   La page **Démarrer ou continuer votre configuration** s'affiche.
7. Sélectionnez **l'option Confirmer que l'ensemble de mises à jour de configuration de signature de code a été importé et validé.** Cochez la case et sélectionnez **Suivant**.
   Sur la page Configuration du contrôle du quorum, examinez les informations que vous avez **saisies et sélectionnez Déclencher l'approbation du quorum**.
8. Dans l'instance protégée, sélectionnez État de **révocation de certification** dans la page Déclencher l'approbation du quorum pour consulter les mises à jour des approbations de demande de contrôle du quorum.
9. **Sélectionnez Détails de l'approbateur** et passez en revue l'état des demandes de quorum.

Approuver la révocation du certificat

Examinez et approuvez les demandes de révocation de certificat à partir des notifications d'approbation par e-mail qui sont envoyées à votre adresse e-mail enregistrée. Examinez la notification d'approbation et sélectionnez le lien **Cliquez ici pour approuver** ou **Cliquez ici pour rejeter** pour accéder à l'instance protégée et agir. Vous pouvez également accéder à la demande d'approbation et à la demande de quorum de signature de code directement à partir de l'e-mail.

Avant de commencer

Rôle requis : sn_cse.codesigning_admin, approver_user

Procédure

1. Accédez à l'instance protégée en cliquant sur les liens fournis dans l'e-mail de notification.
2. Passez en revue les demandes de transaction dans le menu Approbations.
3. Approuvez la tâche en sélectionnant **Approuver**.
4. Sur la page de confirmation d'approbation, sélectionnez **Oui** pour accéder à la demande spécifique de quorum de signature de code.
5. Passez en revue la demande de Signature de code quorum et ajoutez des notes supplémentaires dans le menu **Commentaires** , si nécessaire.
6. Sélectionnez **Mettre à jour**.

Résultats

La Signature de code demande de quorum est approuvée. Si vous avez activé le redémarrage du serveur MID lors de l'exportation de la demande de révocation, le serveur MID redémarre pour que la demande soit activée.

Désactiver la signature de code

Désactivez la signature de code sur votre instance protégée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin, codesigning_admin

Procédure

1. Sur votre instance de confiance, accédez à **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** pour ouvrir la page de configuration de signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **l'instance de confiance**.
3. Sélectionnez le bouton **Suivant** .
4. Dans le champ **Action** , sous **Sélectionnez l'action que vous souhaitez accomplir**, sélectionnez **Désactiver la signature de code**.
5. Dans le panneau **Exporter le fichier de configuration** , sélectionnez **Exporter** pour télécharger l'ensemble de mises à jour.
   Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes suivantes.
6. Sélectionnez **Terminé**.
7. Connectez-vous à votre instance protégée.
8. Chargez vos fichiers de configuration en suivant les étapes de la section Chargez votre fichier de configuration de signature de code sur votre instance protégée.
9. Accédez à la **Tous** > **Signature de code** > **Configuration** > **Configuration guidée** pour ouvrir la page de configuration de signature de code.
10. Dans le champ **Type d'instance** , sélectionnez **Instance protégée**.
11. Sélectionnez le bouton **Suivant** .
12. Cochez la case **Veuillez confirmer que l'ensemble de mises à jour de configuration de signature de code a été importé et validé** .
13. Sélectionnez le bouton **Suivant** .
14. Attendez la fin de l'installation du certificat.
    Une fois l'opération terminée, le message Une **configuration de signature de code terminée avec succès** s'affiche.

Résultats
Vous pouvez vérifier la réussite de l'exécution en consultant les propriétés de votre système. Recherchez la propriété **com.snc.kmf.signature.validation.flag** dans la table Propriétés système [sys_property] et vérifiez que la valeur est **false**.

Charger les paires de clés et les certificats requis pour la signature de code

Établissez la relation dans une instance de confiance désignée à l'aide de la signature de code. Cette première étape charge deux clés cryptographiques dans l'environnement approuvé afin d'établir une source fiable pour les mises à jour de l'instance de production.

Avant de commencer
Rôles requis : security_admin et sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche
La première étape de l'établissement de la relation consiste à établir la base de confiance dans une instance approuvée désignée à l'aide de la signature de code. Pour effectuer cette tâche, vous avez besoin des éléments suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous devez disposer de deux paires de clés publiques/privées RSA 4 096 bits à charger dans les modules cryptographiques de signature de code :
  - Une paire pour le module de chiffrement cm_code_signing
  - Une paire pour le module de chiffrement cm_code_attest

  Pour plus d'informations sur ces touches, reportez-vous à la section Créer des paires de clés et des certificats de signature de code.

  Important :
  Ces paires de clés doivent être signées par une autorité de certification publique ou par l'autorité de certification interne de votre organisation. Le certificat ne peut pas être auto-signé.

- Un fichier de norme de cryptographie à clé publique #12 (.p12) contenant vos certificats feuille et intermédiaire.

Procédure

1. Importez vos clés à partir du magasin de clés.
   a. Accédez à la **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Tous**.
   b. Recherchez et ouvrez le module de chiffrement nommé `cm_code_signing`.
   c. Dans la liste **Spécifications cryptographiques** , sélectionnez le nom de la spécification cryptographique pour l'ouvrir.
   d. Dans l'écran **Importer la clé à partir du magasin de clés** , sélectionnez **Importer la clé**.
2. Répétez la première étape pour importer le module de chiffrement nommé `cm_code_attest`.
3. Dans le champ **Saisir le mot de passe du magasin de clés** , saisissez le mot de passe de défi que vous avez créé lors de la génération de votre certificat RSA.

   Remarque :
   Le mot de passe de défi que vous avez créé est appelé ici le **mot de passe du magasin de clés**. Dans d'autres parties du processus, il peut s'agir d'un **mot de passe d'importation** ou d'un **mot de passe d'exportation**. Dans tous les cas, ce mot de passe est le même que celui que vous avez créé aux étapes précédentes.

4. Sélectionnez le bouton **Parcourir** en regard de **Importer le magasin de clés/certificat**.
5. Sélectionnez un fichier Public Key Cryptography Standard #12 (.p12) contenant votre certificat de distribution (mentionné dans la section avant de commencer en haut de ce document).
6. Sélectionnez **OK**.

   Important :
   Si vous utilisez votre propre autorité de certification interne, vous devez télécharger les certificats intermédiaires de l'autorité de certification interne en suivant le processus des étapes 5 et 6.

   Une fois votre clé et vos certificats importés, un message de confirmation s'affiche.

   Vous pouvez valider que la clé et les certificats sont présents sur votre instance dans la table Certificats X.509 [sys_certificate]. Ces enregistrements ont un type de **certificat de magasin de confiance**.

   Vous pouvez valider votre clé sur la table Modules de chiffrement [sys_kmf_crypto_module].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Exporter le certificat en production. Consultez Préparer les certificats de cercle de confiance pour en savoir plus.

Préparer les certificats de cercle de confiance

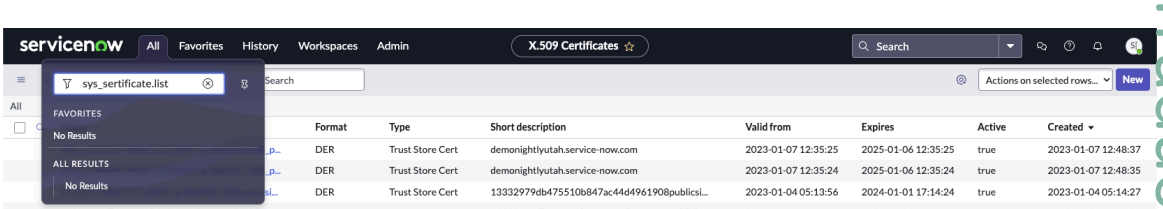
Créez un ensemble de mises à jour dans l'environnement approuvé pour exporter le certificat approuvé vers l'environnement de production.

Avant de commencer
Rôles requis : admin, security_admin

Avant de commencer
Instance de confiance

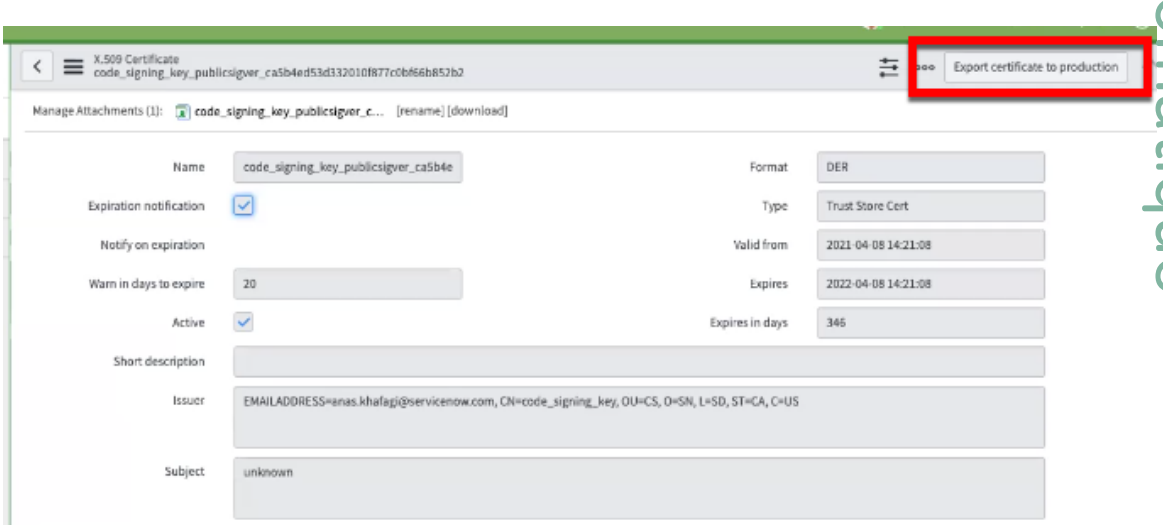
Procédure

1. Dans l'environnement approuvé, accédez à **sys_certificate.liste**.



2. Ouvrez le certificat X.509 le plus récemment créé qui a été généré avec le type **Certificat de magasin de confiance**.
   Vous devrez peut-être ajouter le champ **Créé** à la liste pour trouver l'enregistrement le plus récent. Voir Listes personnelles .

3. Sélectionnez **Exporter le certificat vers la production**.



   Une signature est créée avec le certificat.

4. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.

5. Recherchez et ouvrez la mise à jour de signature de code.

   Cette mise à jour commence par le texte code_signing_key_publicsigver.

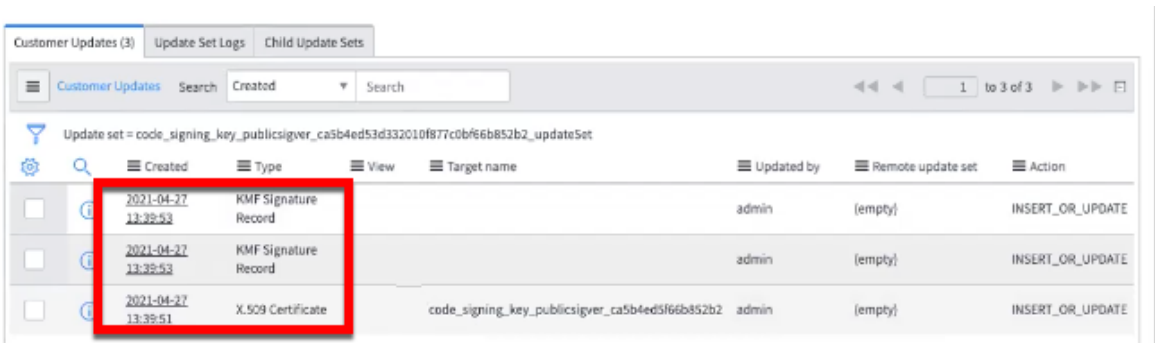
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

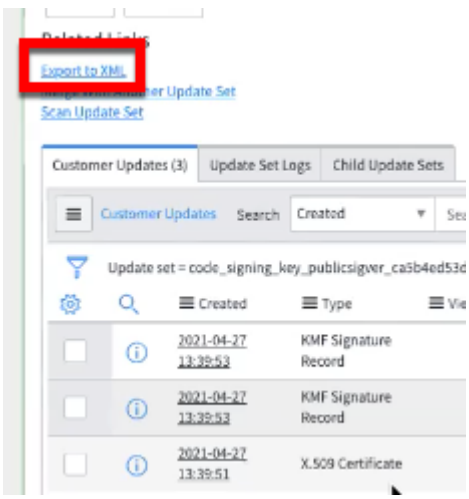
Un nouvel enregistrement d'ensemble de mises à jour de signature de code a été créé par les étapes précédentes. Pour trouver cet enregistrement, triez la liste à l'aide du champ **Créé par** et recherchez les enregistrements dans le champ **Nom** .

6. Affichez les enregistrements de signatures pertinents et le certificat X.509.

   L'ensemble de mises à jour comprend la pièce jointe pour l'enregistrement de signature ainsi que l'entrée de la signature dans la table et le certificat.



7. Sélectionnez le lien connexe **Exporter vers XML** .



8. Récupérez l'ensemble de mises à jour en production.
   Consultez Retrieve an update set pour en savoir plus.

> **Important :**
> Répétez ces étapes pour votre deuxième paire de clés. N'oubliez pas qu'il existe une clé pour les modules cm_code_attest et cm_code_signing cryptographiques.

Importer et installer des certificats pour le cercle de confiance

Récupérez l'ensemble de mises à jour en production pour établir la relation de confiance entre les deux instances. Les certificats qui ont été créés pour représenter la confiance dans l'instance de confiance doivent être acceptés dans l'instance protégée.

Avant de commencer

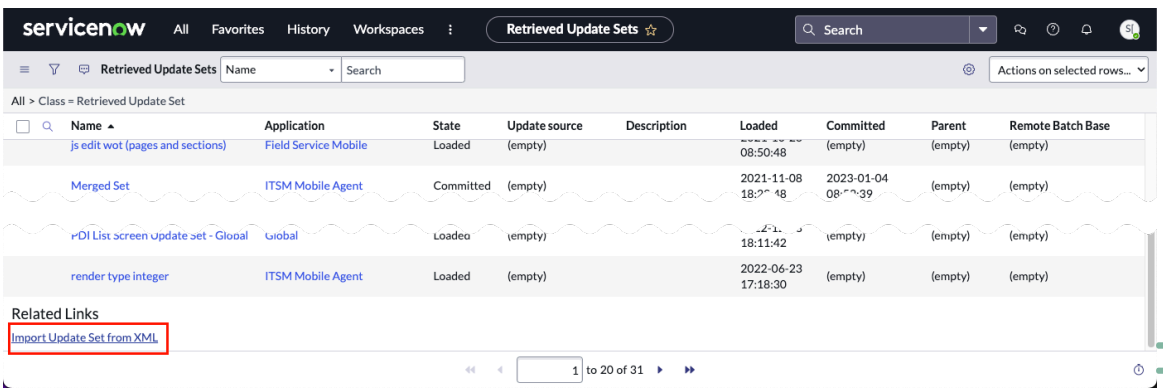
Rôles requis : admin, security_admin

Traduction automatique

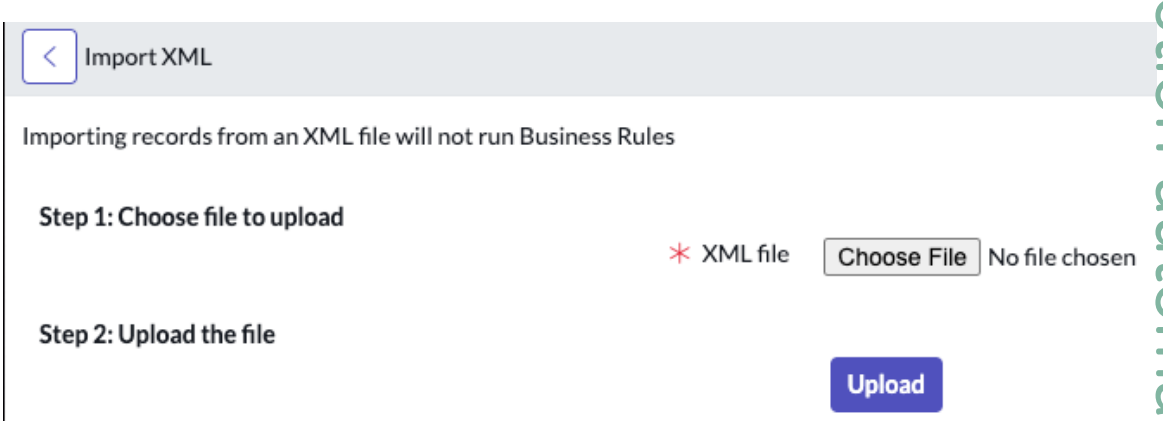
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

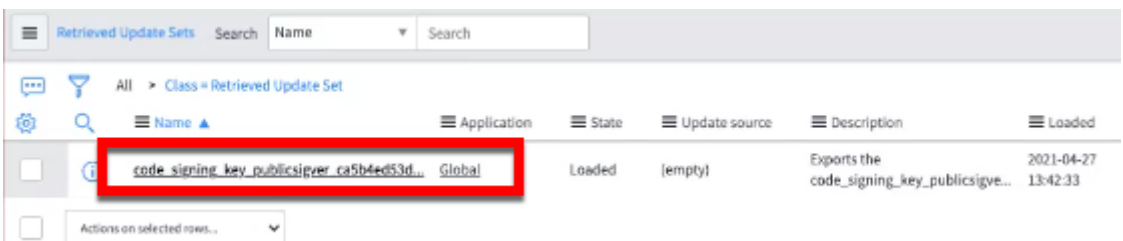
1. Dans l'instance protégée, accédez à **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
2. Sélectionnez le bouton **Importer un ensemble de mises à jour à partir d'un XML** dans le coin inférieur gauche de l'écran.



3. Sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez exporté dans Préparer les certificats de cercle de confiance.



4. Sélectionnez **Charger**.
   L'ensemble de mises à jour de signature de code est ajouté à la table Ensembles de mises à jour récupérés.



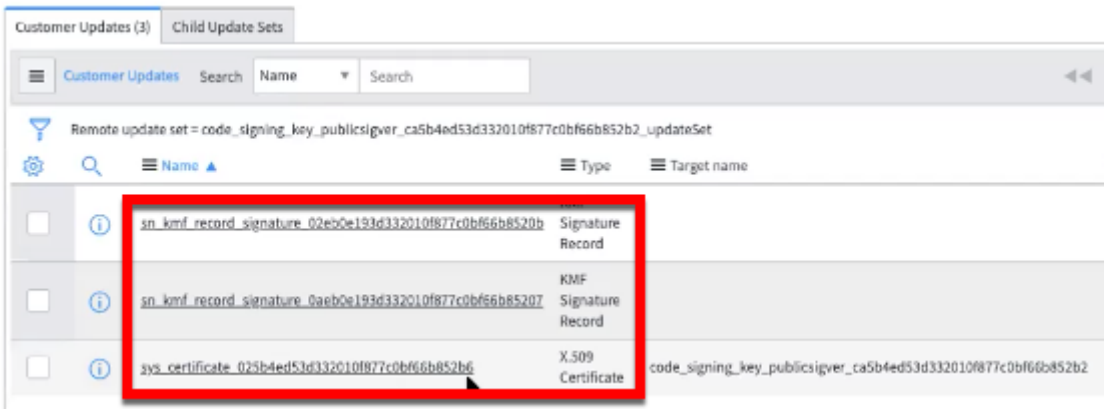
> **Remarque :**
> Si votre ensemble de mises à jour ne s'affiche pas, filtrez votre liste pour les enregistrements à l'état Chargé et triez la liste en fonction du champ **Chargé** .

5. Ouvrez l'enregistrement d'ensemble de mises à jour pour vérifier que la table Mises à jour du client contient les trois enregistrements suivants :

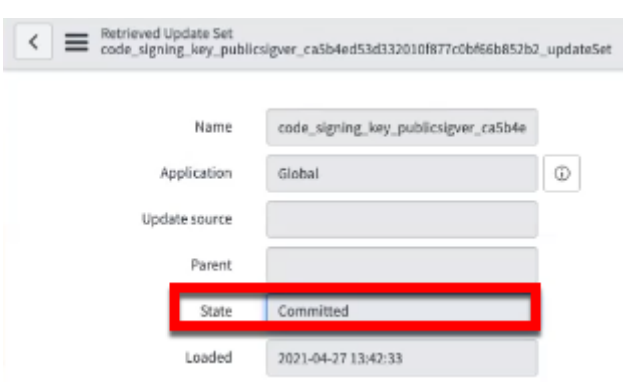
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Deux KMF enregistrements de signature
- Certificat X.509



6. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
7. Sélectionnez **Valider l'ensemble de mises à jour**.

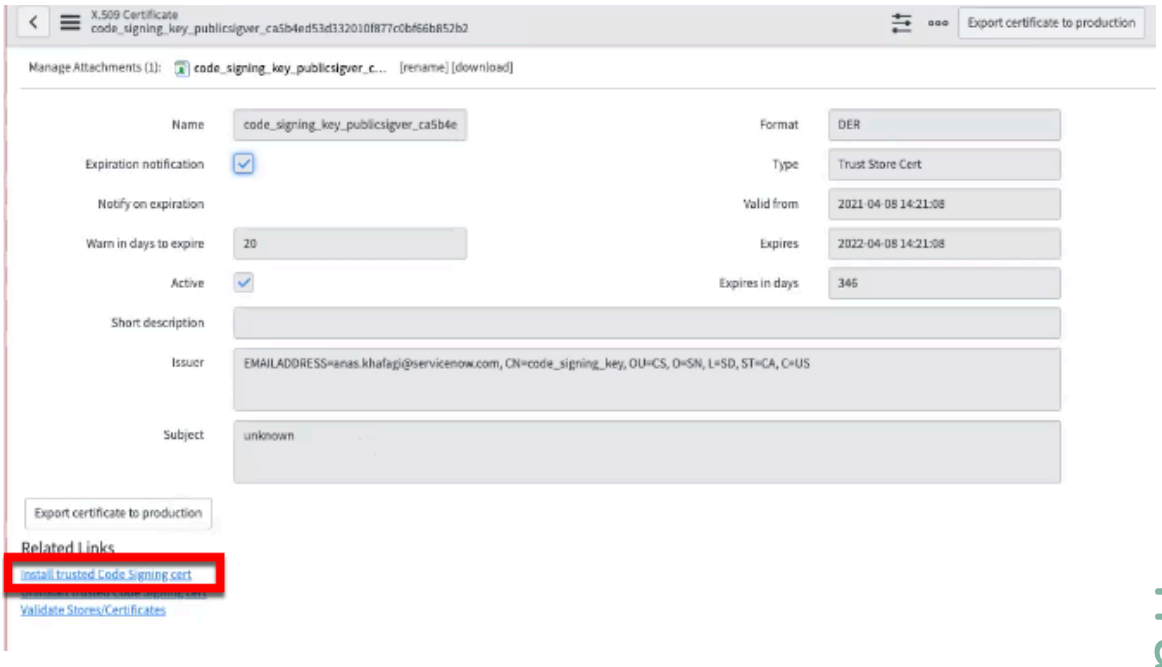


L'état de l'ensemble de mises à jour récupéré est défini sur Validé.

8. Dans le navigateur, saisissez `sn_kmf_record_signature.list` pour ouvrir la liste des **enregistrements de signature KMF** .
9. Localisez les deux KMF enregistrements de signature.
   Ces enregistrements sont les enregistrements les plus récemment créés lorsque le champ **Objet de signature KMF** a une valeur de cercle de confiance. Vous devrez peut-être ajouter le champ **Date de création** à votre liste ou filtrer les enregistrements créés à la date actuelle.
10. Dans le navigateur, saisissez `sys_certificate.list` et ouvrez l'enregistrement avec une valeur Description **brève***de* `code_signing_key` et une valeur **Type** de certificat de magasin de confiance.
11. Sélectionnez **Installer le certificat de signature de code de confiance**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le type de certificat est mis à jour vers `Trusted CodeSigning Cert`.

> **Important :**
> Répétez ces étapes pour votre deuxième certificat. N'oubliez pas qu'il existe un certificat pour les modules cm_code_attest et cm_code_signing cryptographiques.

Résultats

La relation de confiance est établie entre les instances approuvées et protégées. Vous êtes prêt à activer la signature de code. Reportez-vous Activer la signature de code à la section pour terminer les étapes.

Activer la signature de code

Activez la signature de code dans votre instance de non-production approuvée pour identifier les instances approuvées liées à votre instance de production.

Avant de commencer

Rôles requis : security_admin et sn_kmf.crypto_manager ou sn_kmf.admin

En tant qu'administrateur client, vous pouvez accéder au module d'extension Signature de code [com.glide.code_signing_enterprise] et l'installer à partir du portail du module d'extension ServiceNow. Pour en savoir plus sur les cas d'utilisation de la signature de code, reportez-vous à la section Explorer la signature de code.

Pourquoi et quand exécuter cette tâche

Les tâches de signature de code avec des ensembles de mises à jour signés permettent d'activer ou de désactiver la fonctionnalité de signature de code. Il n'y a pas d'autre méthode pour cette fonctionnalité. Ce processus comprend les éléments suivants :

- Créez deux tâches de signature de code dans l'instance approuvée, une pour activer la signature de code et une pour désactiver la signature de code.
  - La tâche planifiée **Activer** démarre le processus de validation du code signé par Serveur MID.
  - La tâche planifiée **Désactiver** arrête la validation du code signé par le Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

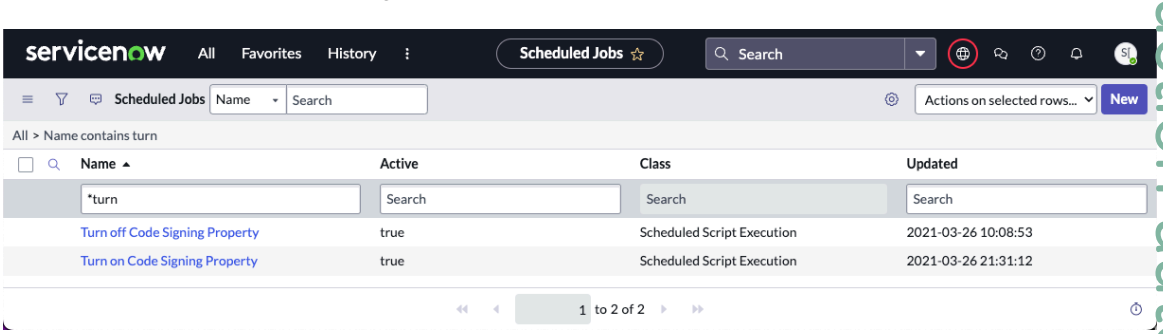
Par défaut, la signature de code s'applique à tous les serveurs MID. Toutefois, si vous devez restreindre la signature de code à un sous-ensemble spécifique de MID Server, vous pouvez le faire à l'aide du pare-feu ECC.

Remarque :
Lorsque vous désactivez la signature de code, la propriété système est marquée comme **fausse**, mais la liste d'amis de confiance pour la signature de code est toujours disponible.

- Placez la tâche **Activer la propriété de signature de code** dans un ensemble de mises à jour.
- Mettez la tâche en production.
- Utilisez le travail **Activer la propriété de signature de code** en production s'il est vérifié que la signature provient d'une instance approuvée.

Procédure

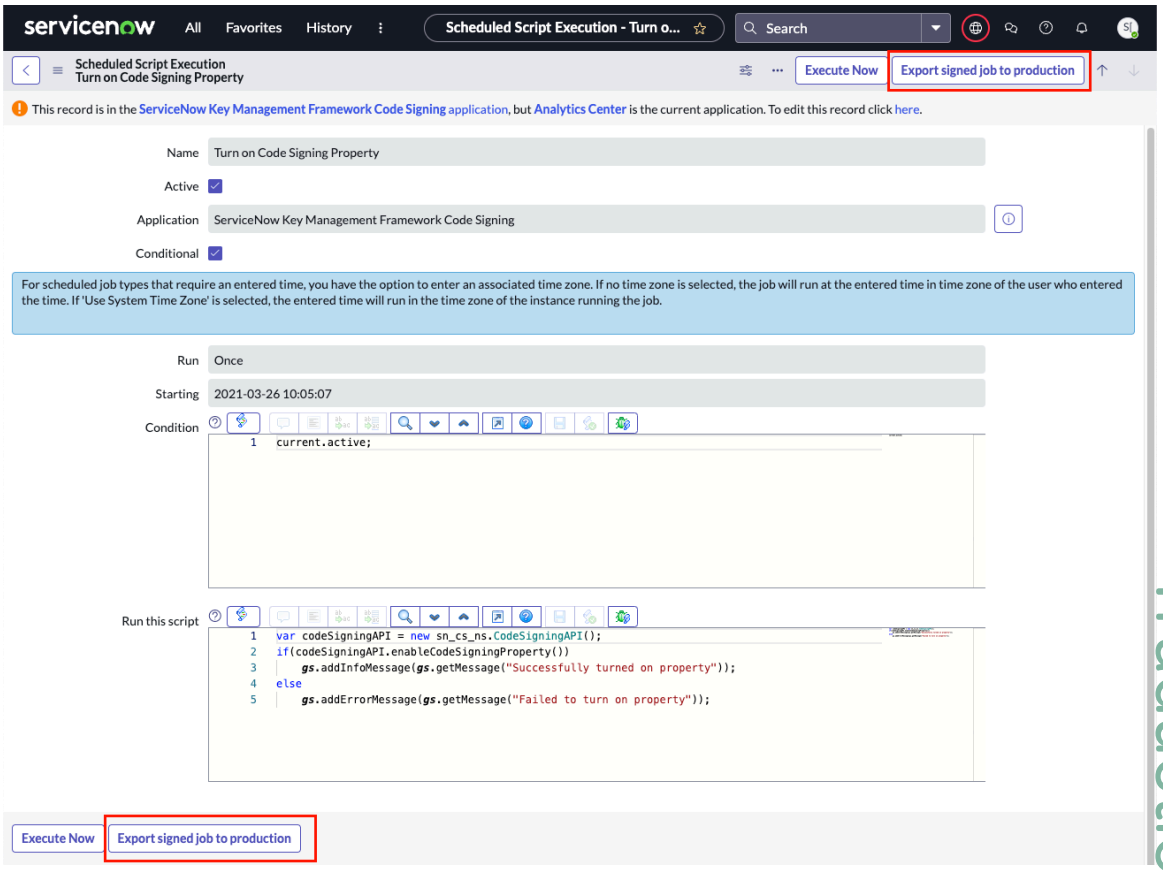
1. Dans votre instance de confiance, accédez à **Tous** > **Définition du système** > **Travaux planifiés**.
2. Recherchez « *Turn » dans le champ de nom.
3. Sélectionnez **Activer la propriété de signature de code**.



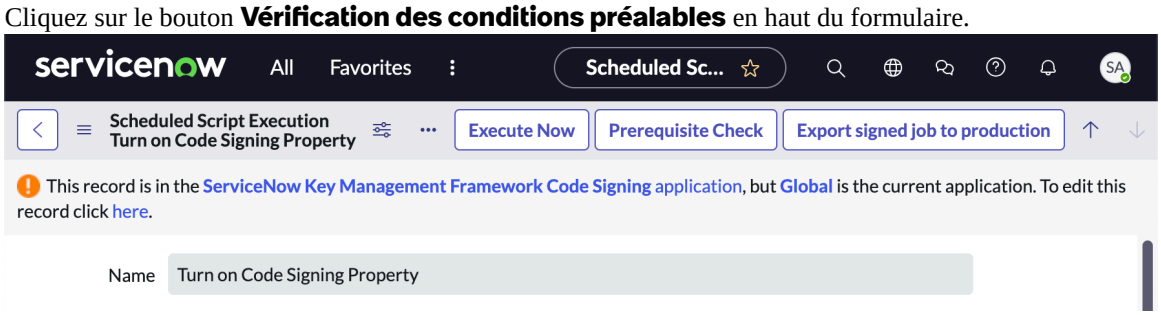
Le formulaire Exécution de script planifiée se charge. Ce formulaire contient des informations permettant d'activer la propriété Signature de code. Les tâches créent des ensembles de mises à jour qui contiennent les tâches et les signatures validées via le processus de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour exécuter le script immédiatement, signez le certificat, créez l'ensemble de mises à jour et sélectionnez **Exporter la tâche signée en production**.
   Vous pouvez également configurer le script pour qu'il s'exécute selon une planification désignée.
5. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
6. Ouvrez chacun des ensembles de mises à jour de la propriété Signature de code et sélectionnez **Exporter au format XML**.
7. Connectez-vous à l'instance de production.
8. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
9. Sélectionnez le bouton **Importer l'ensemble de mises à jour à partir d'un XML** , puis sélectionnez l'ensemble de mises à jour de la propriété Signature de code.
10. Sélectionnez **Choisir un fichier** , puis chargez et validez les ensembles de mises à jour.
11. Revenez à la liste des travaux planifiés en accédant à **Tous** > **Définition du système** > **Travaux planifiés**.
12. Ouvrez l'enregistrement de la **tâche Activer la propriété de signature de code** .
13. Cliquez sur le bouton **Vérification des conditions préalables** en haut du formulaire.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

14. Sélectionnez le bouton **Exécuter maintenant** une fois la vérification des conditions préalables terminée. La tâche planifiée **Activer la propriété de signature de code** lance le processus de validation du code signé par le Serveur MID.
15. Dans le navigateur, saisissez `sn_kmf_record_signature.list` pour ouvrir la liste des **enregistrements de signatures KMF** et filtrer les enregistrements dont l'objectif de **signature KMF** est `le cercle de confiance`.
    La relation de confiance a déplacé les tâches et lorsque les tâches sont utilisées, le processus de vérification de signature s'exécute. Si les tâches, les signatures et les certificats font tous partie de la Cercle de confiance, la signature de code avec Cercle de confiance peut être activée.
16. Dans le navigateur, saisissez `sys_properties.list` pour ouvrir la liste des propriétés système.
17. Recherchez la valeur et *`com_snc_kmf_signature.validation.flag`* assurez-vous que la valeur est définie sur **vrai**.
18. Vérifiez qu'une nouvelle propriété *`com_snc_kmf_signature.validation.certificate`* est répertoriée dans la table.

Propriétés système

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

Utilisez la Cercle de confiance tâche en production pour vérifier la relation de confiance. Aucune tâche directe qui tente de signer du code ne peut être exécutée en production. Consultez la section Configuration de la signature de code pour plus de détails sur les options de configuration.

Créer des paires de clés et des certificats de signature de code

Créez deux paires de clés vers les certificats signés afin d'établir la confiance entre vos instances protégées et approuvées.

Pour établir la confiance entre vos instances, vous devez créer une paire de clés et un certificat pour chacun des modules `cm_code_attest` et `cm_code_signing` cryptographiques.

La création de paires de clés et de certificats se fait à l'aide d'un outil cryptographique installé sur votre appareil local, tel que l'outil OpenSSL. Pour en savoir plus sur cet outil, reportez-vous à la section https://www.openssl.org . Si votre organisation utilise d'autres outils de chiffrement, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

Spécifications de la paire de clés

Les paires de clés que vous créez doivent répondre à ces exigences.

Type	RSA
Longueur de la clé	4096
Algorithme de signature	RSASSA_PKCS1_V1_5_SHA_512

Spécifications du certificat

Les certificats doivent être signés par une autorité de certification publique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Spécifier des règles personnalisées dans le pare-feu ECC

Configurez le pare-feu ECC (External communication Channel) dans votre Serveur MID en spécifiant les règles personnalisées pour autoriser ou rejeter de manière sélective le message entrant et remplacer la configuration de signature de code.

Les administrateurs de sécurité peuvent utiliser les balises de pare-feu ECC pour remplacer la configuration de signature de code et autoriser ou rejeter des opérations spécifiques sur Serveur MID. Ces règles personnalisées doivent être spécifiées dans le fichier YAML situé à l'adresse suivante : agent/boot-config.yaml.

Ces balises sont spécifiques à un protocole. La configuration spécifiée pour la balise parente s'applique à la balise enfant. Par exemple, si le protocole HTTP est autorisé, les protocoles REST et SOAP sont également autorisés. Ce tableau présente les balises parents et enfants disponibles.

Balise parente	Balise enfant
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
JOURNAL SYSTÈME	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
BASES	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DÉCOUVERTE • EVENT_MANAGEMENT

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balise parente	Balise enfant
	• HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTRATION	

Pour configurer les règles personnalisées :

1. Dans , Serveur MID identifiez le fichier boot-config-sample.yaml.
2. Renommez le fichier YAML en boot-config.yaml et déplacez le fichier vers l'emplacement : agent/boot-config.yaml.
3. Dans le fichier YAML, spécifiez les règles personnalisées et enregistrez les modifications. Un exemple de fichier YAML :

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Redémarrez le Serveur MID.

Modifier votre configuration de la racine de confiance

Faites confiance à vos propres certificats et utilisez-les au lieu de vous fier ServiceNow aux certificats de version (par défaut) en changeant pour utiliser votre racine de confiance (ROT). ServiceNow Les composants tels que les includes de script, les règles métier, entre autres, sont signés au moment de la génération à l'aide d'une ServiceNow clé de temps de génération (le certificat de vérification est le ServiceNow certificat de version).

Modification de la racine de confiance

Pour modifier la racine de confiance pour ces signatures d'enregistrements, vous devez suivre le processus de changement de racine de confiance.

- Générez et migrez un nouvel ensemble de signatures pour tous les composants fournis, à l'aide de votre certificat fourni.
- Désactivez la propriété de la racine de confiance à l'aide d'une tâche planifiée.

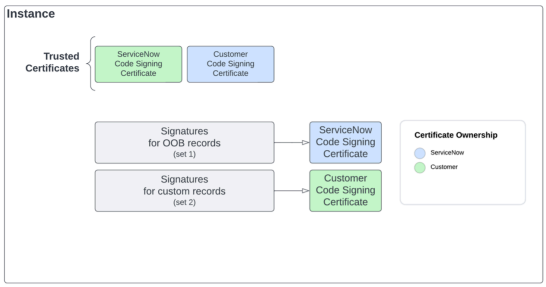
Pour en savoir plus sur ces étapes, consultez Migrer les signatures pour utiliser un certificat client et Désactiver la racine de confiance ServiceNow.

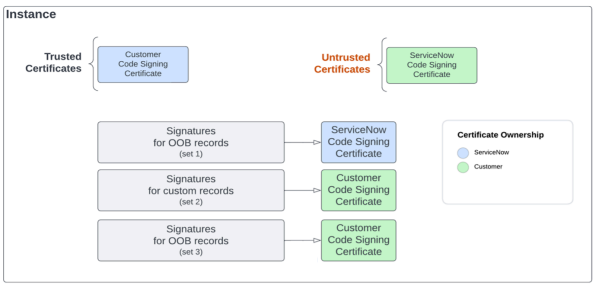
Impact sur le processus de génération et de vérification de signature

Par défaut, les certificats de version de signature de code sont approuvés pendant le processus de vérification de signature. Après avoir effectué ce changement, votre instance accepte uniquement les signatures de votre propre certificat de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Propriété ROT définie sur faux (par défaut)	Propriété ROT définie sur vrai
• Lors de la vérification, les signatures avec des certificats de version sont approuvées. • Lors de la signature, si vous ne fournissez pas de clés, la clé de signature d'instance est utilisée comme clé de secours. • Le point *api/sn_kmf/signature/certificates* de terminaison REST de signature renvoie ServiceNow des certificats de version de signature de code ainsi que d'autres certificats présents sur l'instance.	• Lors de la vérification, les signatures avec des certificats de version ne sont pas approuvées. • Lors de la signature, si vous ne fournissez pas de clés, la signature n'est pas effectuée. • Le point *api/sn_kmf/signature/certificates* de terminaison REST signature exclut les certificats de ServiceNow version (San Diego, Vancouver PKI, W PKI).

Impact sur votre serveur MID

Lorsque la propriété ROT est définie sur faux

Si vous choisissez de conserver votre propriété ROT à sa valeur par défaut (faux), cela n'a aucun impact sur votre serveur MID.

Lorsque la signature de code est activée et que la propriété ROT est définie sur vrai

- L'API *isTrusted()* renvoie la valeur false pour les signatures avec un certificat de version.
- L'API *isTrusted()* renvoie true pour les signatures avec votre certificat.
- L'appel d'API REST pour les certificats exclut les certificats de version.
- Vous pouvez voir des problèmes de Serveur MID, tels que des messages d'échec de validation de signature dans les journaux.

Migrer les signatures pour utiliser un certificat client

Exécutez une tâche de signature pour migrer vos signatures vers une racine de confiance (ROT) client.

Avant de commencer

Rôle requis : admin, security_admin et sn_kmf.cryptographic_manager

La signature de code doit être activée sur vos instances protégées et de confiance. Vous pouvez vérifier que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette procédure fait partie d'une série de procédures permettant de modifier une racine de confiance (ROT) client sur vos instances. Pour une présentation de ce processus, reportez-vous à la section Modifier votre configuration de la racine de confiance.

Procédure

1. Connectez-vous à votre instance protégée.
2. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.
3. Recherchez et ouvrez la tâche **planifiée ROT : générer un ensemble de mises à jour d'enregistrements pour migrer les signatures à l'aide de** la tâche planifiée de certificat client.
4. En bas du formulaire, sélectionnez **Exécuter maintenant**.
5. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
6. À l'invite, sélectionnez **Tâche de signature**.
7. Dans le formulaire **Tâche de signature** , renseignez les champs selon vos besoins.

Champ	Valeur
Nom	Créez un nom unique pour votre tâche.
Type	Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Sélectionnez l'ensemble de mises à jour créé lors des étapes précédentes. Le nom de l'ensemble de mises à jour commence par change_root_of_trust_updateSet.

8. Cliquez avec le bouton droit sur l'en-tête du formulaire et sélectionnez **Enregistrer** pour enregistrer cet enregistrement.
9. Cliquez avec le bouton droit sur l'en-tête du formulaire et sélectionnez **Exporter** > **XML (cet enregistrement)** pour exporter cet enregistrement sous forme de fichier XML.
10. Connectez-vous à votre instance de confiance.
11. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Tous**.
12. Cliquez avec le bouton droit sur l'en-tête de liste, puis sélectionnez **Importer XML**.
13. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé aux étapes précédentes.
14. Sélectionnez **Charger**.
15. À partir de la liste, ouvrez la tâche de sécurité importée.
16. Sélectionnez **Exporter la tâche de signature de code vers la production**.
    Cette action signe la tâche et la place dans un nouvel ensemble de mises à jour que vous pouvez importer dans votre instance protégée.

> **Important :**
> Après avoir signé la tâche, vous devez effectuer les étapes suivantes dans les 10 minutes. Si vous dépassez cette période, vous pouvez signer à nouveau la tâche en suivant ces étapes, ce qui crée un autre ensemble de mises à jour signé.

17. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
18. Recherchez l'ensemble de mises à jour créé lors des étapes précédentes.
    Le nom commence par SIGN_UPDATE_SET_updateSet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

19. Sélectionnez **Exporter XML** pour exporter votre ensemble de mises à jour sous forme de fichier XML.
20. Connectez-vous à votre instance protégée.
21. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
22. En bas de la liste, sélectionnez **Importer un ensemble de mises à jour à partir de XML**.
23. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé aux étapes précédentes.
24. Sélectionnez **Charger**.
25. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**et ouvrez l'ensemble de mises à jour en commençant par SIGN_UPDATE_SET_updateSet.
26. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
27. Une fois l'aperçu terminé, sélectionnez **Valider l'ensemble de mises à jour**.
28. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Tous**.
29. Ouvrez la tâche de sécurité importée.
30. Sélectionnez **Démarrer** pour exécuter la tâche de sécurité.

    Une fois la tâche de sécurité terminée, les informations relatives à l'état de la tâche s'affichent dans le champ **Résumé** .

    Lorsque la tâche est à l'état Terminé, toutes les signatures des enregistrements d'ensemble de mises à jour doivent utiliser le certificat fourni par le client comme certificat de vérification. Vous pouvez le vérifier sur la table Enregistrements de signature KMF [sn_kmf_record_signature].

Que faire ensuite

Pour poursuivre le processus de configuration de la racine de confiance, reportez-vous à la section Désactiver la racine de confiance ServiceNow.

Désactiver la racine de confiance ServiceNow

Exécutez une tâche planifiée sur votre instance de confiance pour désactiver la racine de confiance.

Avant de commencer

Rôle requis : admin, security_admin et sn_kmf.cryptographic_manager

La signature de code doit être activée sur vos instances protégées et de confiance. Vous pouvez vérifier que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur vrai.

Cette procédure fait partie d'une série de procédures permettant de passer à une racine de confiance client (ROT) sur vos instances. Pour une présentation de ce processus, reportez-vous à la section Modifier votre configuration de la racine de confiance.

Procédure

1. Connectez-vous à votre instance de confiance.
2. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.
3. Ouvrez la tâche planifiée **Désactiver la racine de confiance ServiceNow** .
4. Sélectionnez **l'option Exporter la tâche signée vers la production**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
6. Recherchez et ouvrez l'ensemble de mises à jour **Désactiver la racine de confiance ServiceNow** .
7. Sélectionnez **Exporter XML** pour exporter votre ensemble de mises à jour sous forme de fichier XML.
8. Connectez-vous à votre instance protégée.
9. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
10. En bas de la liste, sélectionnez **Importer un ensemble de mises à jour à partir de XML**.
11. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé aux étapes précédentes.
12. Sélectionnez **Charger**.
13. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**et ouvrez l'ensemble de mises à jour **Désactiver la racine de confiance ServiceNow** .
14. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
15. Une fois l'aperçu terminé, sélectionnez **Valider l'ensemble de mises à jour**.
16. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.
17. Ouvrez la tâche planifiée importée dans l'ensemble de mises à jour.
18. Sélectionnez le bouton **Exécuter maintenant** pour exécuter la tâche.

Résultats

L'exécution du travail planifié définit la propriété ROT sur true. Votre instance est configurée pour utiliser la racine de confiance client.

Utilisation de la signature de code

Découvrez comment signer des enregistrements, des messages et des pièces jointes pour vérifier l'authenticité et l'intégrité de vos données.

Signer les enregistrements de source de données JDBC dans l'instance protégée

Utilisez des ensembles de mises à jour pour signer et valider les sources de données JDBC en activant la signature de code dans les instances protégées et approuvées.

Signer les messages REST et SOAP dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les messages REST et SOAP en activant la signature de code dans les instances protégées et de confiance.

Signer les flux, les flux secondaires et les actions dans l'instance protégée

Utilisez des ensembles de mises à jour pour signer et valider les flux, les flux secondaires et les actions en activant la signature de code dans les instances protégées et de confiance.

Signer des enregistrements ou des pièces jointes spécifiques

Créez une tâche de sécurité pour signer des enregistrements ou des pièces jointes spécifiques plutôt que tous les enregistrements ou pièces jointes d'une table.

Outil de signature autonome

Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans les applications à ServiceNow l'aide de votre propre clé privée.

Traduction automatique

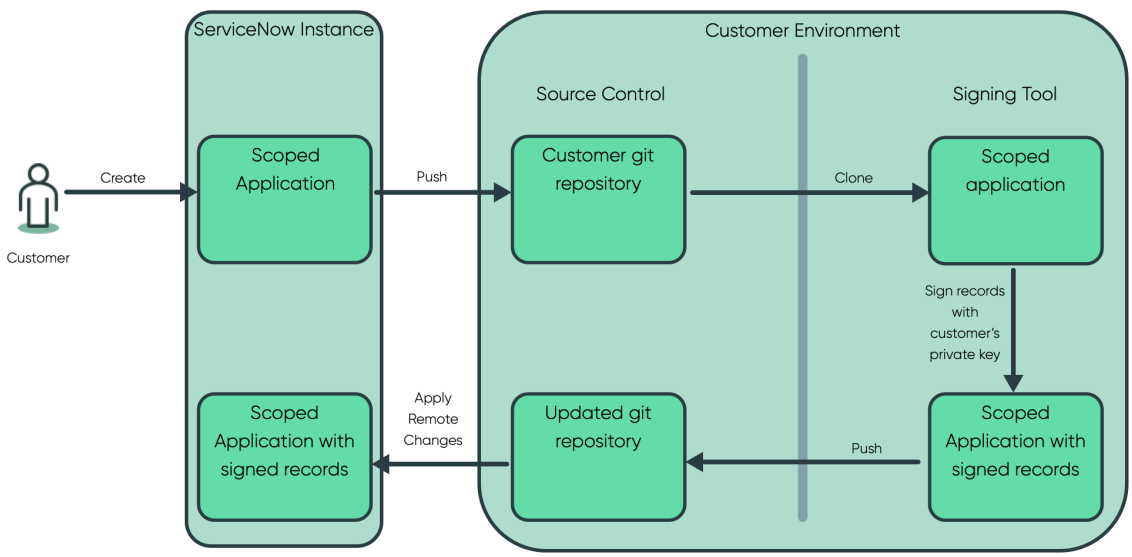
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Outil de signature autonome

Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans les applications à ServiceNow l'aide de votre propre clé privée.

Utilisez l'outil de signature pour signer les enregistrements dans ServiceNow les applications. L'outil génère des signatures pour les enregistrements de votre environnement local à l'aide de votre propre clé privée.

Workflow de l'outil de signature



1. Créez ou sélectionnez une application existante ServiceNow avec des enregistrements à signer, tels que des règles métier ou des includes de script.
2. Poussez l'application dans votre référentiel Git, qui se trouve dans votre environnement.

> **Remarque :**
> Les applications peuvent être synchronisées entre un référentiel Git et votre instance à l'aide de l'intégration du contrôle de source. Pour en savoir plus sur la configuration et l'utilisation de cette intégration, reportez-vous à la rubrique Legacy - Source Control integration .

3. Clonez l'application dans votre environnement local.
4. Utilisez l'outil de signature (également dans votre environnement local) pour signer les enregistrements pris en charge à partir de l'application clonée ServiceNow à l'aide de votre clé privée. L'outil de signature crée des enregistrements de signatures et des enregistrements de certificat X.509 [sys_certificate]. Pour plus d'informations sur l'utilisation de l'outil de signature, reportez-vous à la section Utilisation de l'outil de signature.
5. Transmettre par push l'application mise à jour à votre référentiel Git.
6. Dans votre instance, importez l'application mise à jour en appliquant des changements distants.

Utilisation de l'outil de signature

Découvrez comment utiliser l'outil de signature pour signer les enregistrements pris en charge dans les ServiceNow applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Pour effectuer ces étapes, vous devez disposer des éléments suivants :

- Une ServiceNow application qui a des enregistrements à signer.
- Une clé privée pour signer les enregistrements.
- Le script *signRecords.sh* dans votre environnement local, avec autorisation d'exécution.

> **Important :**
> Le script *signRecords.sh* est inclus dans le fichier jar de l'outil de signature, que vous devez demander à ServiceNow Service clientèle .

Procédure

1. Dans votre environnement local, accédez au répertoire contenant le script *signRecords.sh* .
2. Utilisez le format de commande suivant pour signer vos enregistrements :

   ```
   ./signRecords.sh -d [Path to the root directory of the ServiceNow Application to Sign] -f [Path to the Keystore file]
   ```

   Par exemple :

   ```
   ./signRecords.sh -d /users/abc/ServiceNow-App-1 -f /users/abc/codesigning.p12
   ```

3. Si vous y êtes invité, saisissez le mot de passe du magasin de clés.
   Appuyez sur Entrée s'il n'y a pas de mot de passe.
4. Examinez la sortie pour confirmer que la signature a réussi.

   ```
   Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: executing codesigning...
   Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
   INFO: CODESIGN: signing record for documentId: 65e811327702111057416efe7c5a994f
   Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: codesigning successfully completed!
   ```

   Dans l'exemple de sortie précédent, l'outil de signature a utilisé le fichier de magasin de clés fourni pour signer l'enregistrement. Vous pouvez également voir que :

   - Le script a trouvé un `65e811327702111057416efe7c5a994f` d'enregistrement pris en charge et l'a signé.
   - Dans le répertoire ServiceNow-App-1, deux enregistrements sont créés : `sys_certificate.xml` et `sn_kmf_record_signature.xml`.

5. Importez à nouveau l'application mise à jour dans votre instance en appliquant des modifications distantes dans Studio.
   Pour plus d'informations, consultez Legacy - Apply remote changes .

Arguments de l'outil de signature

Découvrez les arguments disponibles pour l'outil de signature.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Arguments de ligne de commande

Argument	Obligatoire	Description
-d	Oui	Répertoire racine du projet à signer. Doit contenir un répertoire de projet (aléatoire 32 caractères alphanumériques), un fichier sn_source_control.properties et un fichier <project_name>.iml
-f	Oui	Chemin d'accès au magasin de clés.
-a	Non	Alias utilisé pour accéder à une entrée spécifique dans le magasin de clés.
-c	Non	Concaténer les signatures d'enregistrement dans un seul fichier.
-k	Non	Mot de passe permettant d'accéder à la clé stockée dans le magasin de clés. Vous pouvez également saisir ce mot de passe lorsque vous y êtes invité et non dans l'argument.
-o	Non	Signez avec un nouveau certificat à la place de tous les fichiers sys_cert existants.
-p	Non	Mot de passe permettant d'accéder au magasin de clés s'il possède un mot de passe. Vous pouvez également saisir ce mot de passe lorsque vous y êtes invité et non dans l'argument.
-w	Non	Effacer tous les fichiers d'enregistrement de signature existants.
-h	Non	Affichez ce message d'aide et quittez.

Signer les enregistrements de source de données JDBC dans l'instance protégée

Utilisez des ensembles de mises à jour pour signer et valider les sources de données JDBC en activant la signature de code dans les instances protégées et approuvées.

- Établissez Cercle de confiance entre les instances protégées et approuvées.
- Rôle requis : sécurité_admin

Remarque :

- Serveur MID ne gère pas les sources de données du fichier et, par conséquent, ces sources de données ne sont pas signées par code.
- Les sources de données LDAP ne peuvent pas être signées par code.

Signer les sources de données existantes de type JDBC

Utilisez des ensembles de mises à jour pour apporter des tâches de signature en masse à l'instance protégée.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Dans l'instance approuvée, configurez la tâche de signature KMF pour signer les sources de données.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

b. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer en masse les enregistrements**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionnez **une source de données**.

d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
Un message de confirmation s'affiche pour indiquer que l'ensemble de mises à jour est signé.

e. Exporter l'ensemble de mises à jour généré dans un fichier XML.

2. Dans l'instance protégée, importez et validez l'ensemble de mises à jour pour récupérer les travaux signés en masse à partir de l'instance de confiance.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

b. Ouvrez l'ensemble de mises à jour exporté à partir de l'instance de confiance.

c. Cliquez sur **Démarrer**.
Un message de confirmation s'affiche pour indiquer que les enregistrements sont signés.

Signer les nouvelles sources de données de type JDBC

Utilisez des ensembles de mises à jour pour apporter l'ensemble de mises à jour signé à l'instance protégée.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

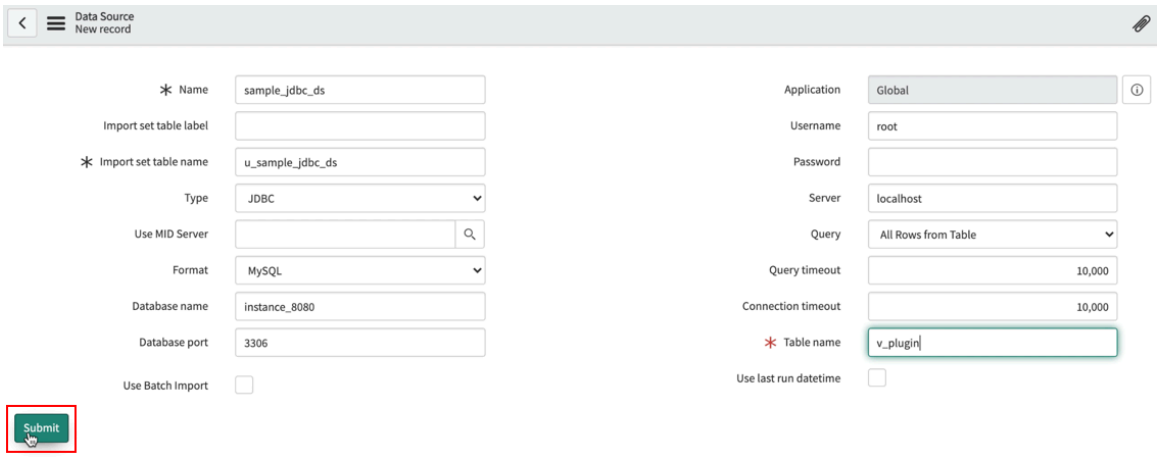
1. Dans l'instance approuvée, démarrez un ensemble de mises à jour.



2. Dans l'instance approuvée, créez les sources de données requises.

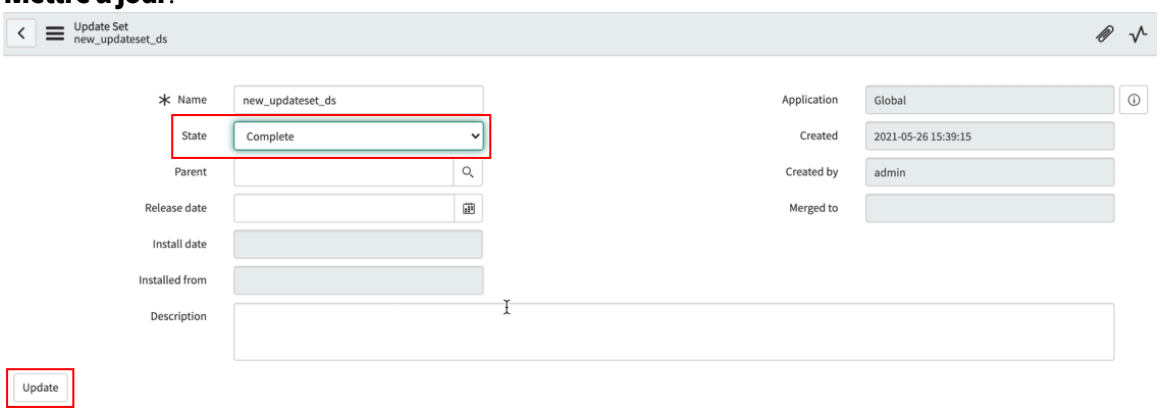
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les sources de données sont ajoutées à l'ensemble de mises à jour.

3. Dans l'instance de confiance, définissez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.



4. Dans l'instance approuvée, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

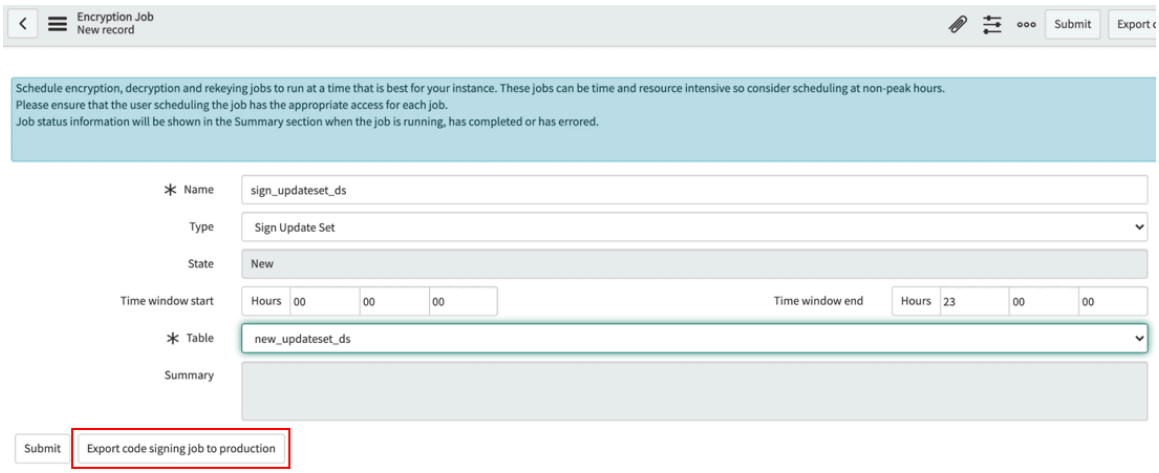
   b. Cliquez sur **Nouveau**.

   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés.

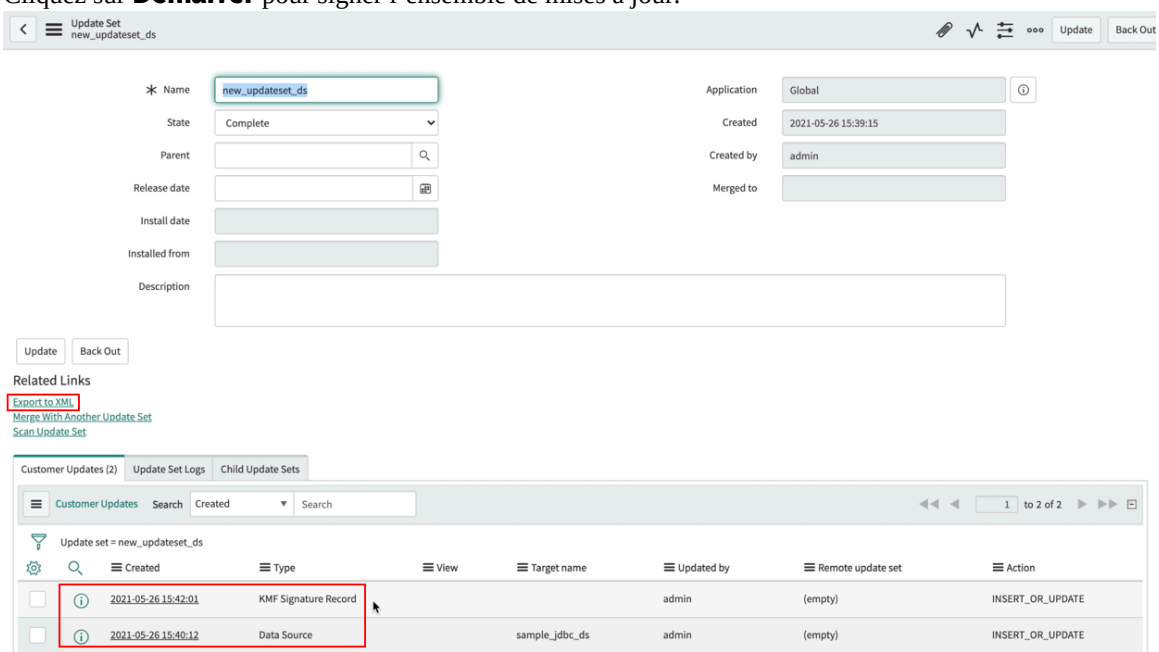
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Cliquez sur **Envoyer**.

e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.



- **Le résumé** est mis à jour pour indiquer que les enregistrements sont signés.
- L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance approuvée, ouvrez l'enregistrement de l'ensemble de mises à jour signé et exportez-le vers un format XML.

6. Dans l'instance protégée, importez l'ensemble de mises à jour signé.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer l'ensemble de mises à jour à partir d'un XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signer les messages REST et SOAP dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les messages REST et SOAP en activant la signature de code dans les instances protégées et de confiance.

Avant de commencer

- Établissez Cercle de confiance entre les instances protégées et approuvées.
- Rôle requis : security_admin

Signez les messages REST et SOAP existants

Signez et validez les messages REST et SOAP existants en activant la signature de code dans les instances protégées et de confiance.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance approuvée, configurez la tâche de signature KMF pour signer les actions d'interface utilisateur.

   a. Accédez à la configuration de signature KMF.

   b. Renseignez ces valeurs sur le formulaire.

   Formulaire Configuration de signature KMF

Champ	Description
Nom de la table	Nom de la table Glide. Par exemple, sélectionnez **Actions d'interface utilisateur [sys_ui_action].**
Objectif de signature KMF	Objet de la signature des enregistrements. **Sélectionnez une file d'attente ECC**.
Champs de génération de signature	Champs dans la source de données que vous souhaitez signer. Si des modifications sont apportées aux valeurs d'un ou plusieurs de ces champs, la signature générée précédemment devient non valide. Sélectionnez **le nom** et **le script**.
Filtre de génération de signature	Critères de filtre qui doivent être remplis pour signer les enregistrements.
Signer la pièce jointe	Option permettant de signer la pièce jointe dans l'enregistrement Glide.
Clé d'instance	Option permettant d'utiliser la clé d'instance.

   c. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

2. Dans l'instance approuvée, signez les enregistrements requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

b. Cliquez sur **Nouveau**.

c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer en masse les enregistrements**.
Table	Table à partir de laquelle les enregistrements doivent être signés. **Sélectionnez Action d'interface utilisateur**.

d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
Deux ensembles de mises à jour signés localement sont créés.

- Un ensemble de mises à jour pour la configuration de l'action d'interface utilisateur.
- Un autre ensemble de mises à jour de la tâche de chiffrement pour exporter la tâche de signature de code.

3. Dans l'instance approuvée, exportez l'ensemble de mises à jour local vers un fichier XML.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.

b. Ouvrez l'ensemble de mises à jour que vous avez créé pour la signature en masse des enregistrements.

c. Cliquez sur le lien connexe **Exporter vers XML** et enregistrez le fichier XML.

4. Dans l'instance protégée, importez les ensembles de mises à jour.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer l'ensemble de mises à jour à partir d'un XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

5. Dans l'instance protégée, exécutez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée en sélectionnant **Démarrer**.
Un message de confirmation s'affiche et indique que les enregistrements sont signés.

Signer les nouveaux messages REST et SOAP

Signez et validez les nouveaux messages REST et SOAP de l'instance de confiance en activant la signature de code dans les instances protégées et de confiance.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans l'instance approuvée, démarrez un ensemble de mises à jour.
2. Dans l'instance approuvée, créez les messages REST ou SOAP requis.
   Les messages sont ajoutés à l'ensemble de mises à jour.
3. Dans l'instance de confiance, définissez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.
4. Dans l'instance approuvée, signez l'ensemble de mises à jour en créant une tâche de chiffrement.
   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.
   b. Cliquez sur **Nouveau**.
   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés. Sélectionnez **Signer le nouvel ensemble de mises à jour Rest V2 : 1**.

   d. Cliquez sur **Envoyer**.
   e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.
      - **Le résumé** est mis à jour pour indiquer que les enregistrements sont signés.
      - L'ensemble de mises à jour est mis à jour et inclut la signature.
5. Dans l'instance approuvée, ouvrez l'enregistrement de l'ensemble de mises à jour signé et exportez-le vers un format XML.
6. Dans l'instance protégée, importez l'ensemble de mises à jour.
   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
   b. Sélectionnez le lien connexe **Importer un ensemble de mises à jour à partir d'un XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
   Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
   L'ensemble de mises à jour est validé avec succès.

Signer des enregistrements ou des pièces jointes spécifiques

Créez une tâche de sécurité pour signer des enregistrements ou des pièces jointes spécifiques plutôt que tous les enregistrements ou pièces jointes d'une table.

À partir de la Vancouver version, les administrateurs de sécurité peuvent utiliser des tâches de sécurité pour signer des enregistrements spécifiques sur une table plutôt que tous les

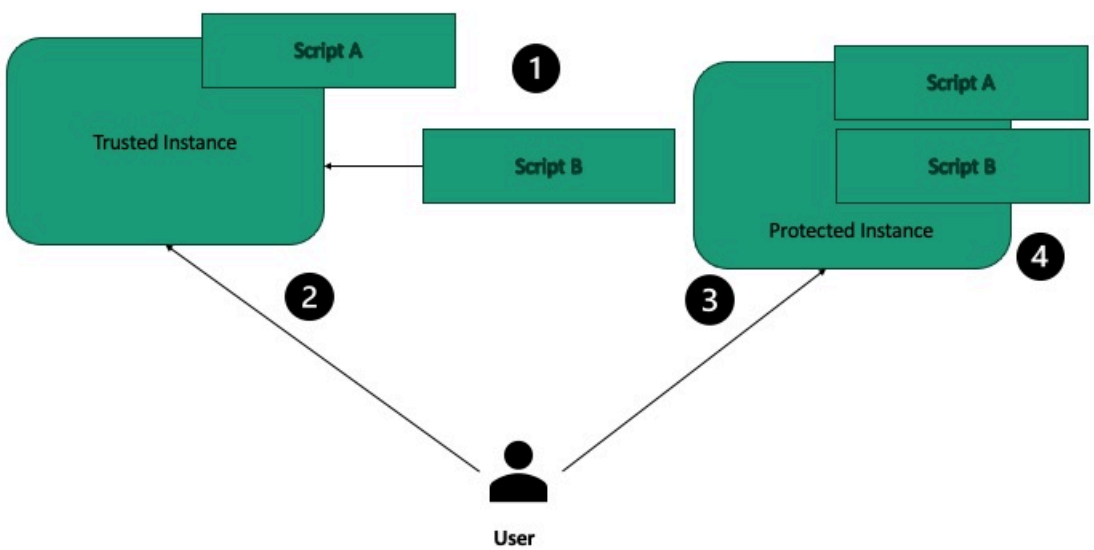
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

enregistrements d'une table. Signez des enregistrements spécifiques pour éviter de signer accidentellement un code non révisé.

Ces tâches incluent un fichier journal joint, qui est généré à la fin de la tâche de signature. Ce fichier journal contient des informations sur les enregistrements signés et la configuration de signature utilisée.

Processus de signature



Ce diagramme montre un exemple d'utilisation du processus de signature. Dans cet exemple, un script, étiqueté Script B , existe uniquement sur l'instance protégée et doit être importé vers une instance de confiance pour être signé. Le script A existe déjà sur les deux instances, il n'est pas nécessaire de le signer. Soit il a déjà été examiné et signé, soit il ne l'a pas encore été et ne devrait pas être signé.

1. Importez l'enregistrement dans votre environnement de confiance.
2. Dans l'instance approuvée, créez une tâche de signature pour signer l'enregistrement. Ce processus est détaillé dans .Créer une tâche pour signer des enregistrements ou des pièces jointes spécifiques sur une instance de confiance
3. Importez la tâche de signature signée dans votre instance protégée à l'aide d'un ensemble de mises à jour.
4. Dans l'instance protégée, exécutez la tâche de signature importée.

Créer une tâche pour signer des enregistrements ou des pièces jointes spécifiques sur une instance de confiance

Signez un enregistrement spécifique ou un groupe d'enregistrements que vous définissez sur une instance de confiance.

Avant de commencer

Rôle requis : security_admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de signature**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un nouvel enregistrement **de tâche de signature** s'affiche.

3. Dans le formulaire, renseignez les champs selon vos besoins :

Champs de tâches de signature

Champ	Description
Nom	Nom descriptif de cette tâche.
Type	Type de tâche de sécurité. Pour signer des enregistrements spécifiques, sélectionnez l'option **Signer des enregistrements spécifiques** . Pour signer des pièces jointes spécifiques, sélectionnez **Signer des pièces jointes spécifiques**.
État	État de cette tâche. Ce champ commence par la valeur **Nouveau**. Ce champ est en lecture seule.
Table	Table contenant les enregistrements ou pièces jointes que vous souhaitez signer. Si vous signez des pièces jointes, sélectionnez la table contenant les enregistrements auxquels les pièces jointes sont associées, et non la table Pièce jointe [sys_attachment]. **Conseil :** Vérifiez la table Enregistrement de signature [sn_kmf_record_signature] du Cadre de gestion des clés (KMF) pour vous assurer qu'il n'y a pas déjà de signatures pour la table que vous avez sélectionnée.
Filtrer les enregistrements	Conditions de filtre utilisées pour limiter les enregistrements qui apparaissent dans la table **Sélectionner les enregistrements pour la signature** .
Sélectionner les enregistrements à signer	Liste des enregistrements de la table sélectionnée dans le champ **Table** , limitée par le filtre créé dans le champ **Enregistrements de filtre** . Déplacez les enregistrements de la fenêtre **Disponible** vers la fenêtre **Sélectionné** pour les inclure dans la tâche de signature.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ. Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.
Fin de la fenêtre de temps	La fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, elle sera mise en pause et reprendra au début de la fenêtre d'heure suivante. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.

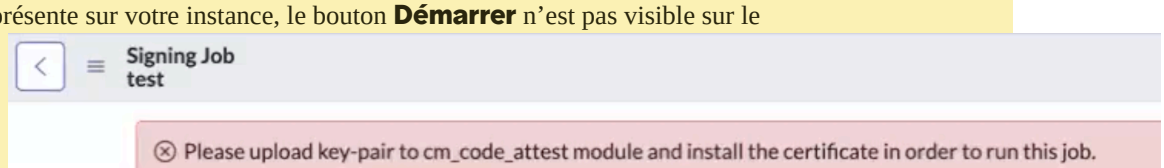
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Résumé	Résumé de l’exécution de cette tâche. Ce champ est en lecture seule.

4. Cliquez avec le bouton droit sur l’en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. En bas du formulaire, sélectionnez **Exporter la tâche de signature de code vers la production**.
   Cette action signe la tâche de signature et elle est prête pour l’exportation.
6. Accédez à la **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**
7. Recherchez et ouvrez l’ensemble de mises à jour pour votre tâche de signature.
   Dans l’onglet Mises à jour du client, vous pouvez voir que cet ensemble de mises à jour inclut la tâche de signature et l’enregistrement de signature.
8. Sélectionnez **Exporter en XML**.
   Cette action crée un fichier XML contenant votre ensemble de mises à jour sur votre appareil local.
9. Sur votre instance de production, accédez à **Tous** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés** > **.**
10. En bas de la page, sélectionnez **Importer un ensemble de mises à jour à partir de XML**.
11. Sélectionnez le bouton **Choisir un fichier** , puis sélectionnez le fichier XML créé lors des étapes précédentes.
12. Sélectionnez **Charger**.
    Votre ensemble de mises à jour est chargé et apparaît dans la liste **Ensembles de mises à jour récupérés** .
13. Dans la liste **Ensembles de mises à jour récupérés** , ouvrez l’enregistrement de votre ensemble de mises à jour importé.
14. Sélectionnez le bouton **Aperçu de l’ensemble de mises à jour** .
    Une fois l’aperçu terminé, vous verrez apparaître le bouton **Valider l’ensemble de mises à jour** .
15. Sélectionnez **Valider l’ensemble de mises à jour**.
16. **Tous** > **Sécurité de système** > **Tâches de Sécurité** > **Tous**.
17. Ouvrez votre tâche de signature.
18. Sélectionnez **Démarrer** pour exécuter la tâche de signature.

> ⚠ **Avertissement :**
> Si la paire de clés n’a pas été téléchargée sur votre instance de production, un avertissement s’affiche en haut du formulaire d’enregistrement. Si cette paire de clés n’est pas présente sur votre instance, le bouton **Démarrer** n’est pas visible sur le formulaire.



Que faire ensuite

Une fois terminé, le champ **Résumé** affiche les résultats de la tâche. Un fichier journal est également joint à votre enregistrement de tâche de signature nommé « Mass_Sign_Records-<sys_id> ». Examinez cet enregistrement pour obtenir des détails sur la tâche et une liste de sys_ids pour chaque enregistrement signé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signer les flux, les flux secondaires et les actions dans l'instance protégée

Utilisez des ensembles de mises à jour pour signer et valider les flux, les flux secondaires et les actions en activant la signature de code dans les instances protégées et de confiance.

- Établissez Cercle de confiance entre les instances protégées et approuvées.
- Rôle requis : security_admin

Signer le flux, les flux secondaires et les actions existants

Signez et validez le flux, les flux secondaires et les actions existants en activant la signature de code dans les instances de production et de confiance.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de confiance, signez les enregistrements dans la table Instance d'étape.
   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.
   b. Cliquez sur **Nouveau**.
   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer en masse les enregistrements**.
Table	Table à partir de laquelle les enregistrements doivent être signés. **Sélectionnez l'instance de l'étape**.

   d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
   Deux ensembles de mises à jour signés localement sont créés.
   - Un ensemble de mises à jour pour la signature KMF.
   - Un autre ensemble de mises à jour de la tâche de chiffrement pour exporter la tâche de signature de code.
2. Dans l'instance approuvée, exportez l'ensemble de mises à jour local vers un fichier XML.
   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
   b. Ouvrez l'ensemble de mises à jour que vous avez créé pour la signature en masse des enregistrements.
   c. Cliquez sur le lien connexe **Exporter vers XML** et enregistrez le fichier XML.
3. Dans l'instance protégée, importez le fichier XML.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer l'ensemble de mises à jour à partir d'un XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

4. Dans l'instance protégée, exécutez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

b. Ouvrez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée.

c. Cliquez sur **Démarrer** pour démarrer la tâche.
Un message de confirmation s'affiche et indique que les enregistrements sont signés.

Signer un nouveau flux, des flux secondaires et des actions

Signez et validez de nouveaux flux, flux secondaires et actions en activant la signature de code dans les instances protégées et de confiance.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance approuvée, démarrez un ensemble de mises à jour.
2. Dans l'instance approuvée, créez les flux, flux secondaires ou actions requis et publiez-les.
Les flux, les flux secondaires ou les actions sont ajoutés à l'ensemble de mises à jour.
3. Dans l'instance de confiance, définissez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.
4. Dans l'instance approuvée, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tous**.

b. Cliquez sur **Nouveau**.

c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés.

d. Cliquez sur **Envoyer**.

e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Le résumé** est mis à jour pour indiquer que les enregistrements sont signés.
- L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance approuvée, ouvrez l'enregistrement de l'ensemble de mises à jour signé et exportez-le vers un format XML.
6. Dans l'instance protégée, importez l'ensemble de mises à jour signé.
   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
   b. Sélectionnez le lien connexe **Importer un ensemble de mises à jour à partir d'un XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
   Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
   L'ensemble de mises à jour est validé avec succès.

Tableau de bord d'intégrité et d'état de signature de code

Le Signature de code tableau de bord d'intégrité et d'état fournit une vue centralisée et conviviale de l'intégrité et de la configuration de votre Signature de code environnement. Utilisez-le pour identifier les problèmes, vérifier l'exactitude de la configuration et prendre en charge des opérations de signature de code sécurisées et ininterrompues.

Le Signature de code tableau de bord d'intégrité et d'état met en évidence les problèmes de configuration et inclut des conseils intuitifs pour vous aider à les résoudre rapidement, réduisant ainsi le besoin d'escalade. Vous pouvez utiliser le tableau de bord pour vérifier que les configurations sont configurées correctement et fonctionnent Signature de code en toute sécurité. Il vous aide à identifier les problèmes potentiels qui pourraient entraîner des échecs et vous permet de fournir des conseils précis aux personnes concernées.

Le tableau de bord vous permet de rechercher, filtrer et analyser à nouveau les paramètres suivants :

- Configurations
- État du certificat
- Détails du module d'extension
- Certificat de vérification de signature
- Configuration de Serveur MID

Pour accéder au tableau de bord d'état et d'intégrité de signature de code, accédez à **Tous** > **Signature de code** > **Intégrité du système** > **Tableau de bord**.

Aperçu du tableau de bord

Le tableau de bord Vue d'ensemble fournit une vue centralisée de votre Signature de code environnement, offrant des informations en temps réel sur les composants clés et leur état.

Le tableau de bord Vue d'ensemble affiche les rapports suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du tableau de bord

Titre	Type	Description
Module d’extension Enterprise	Champ de texte	État des modules d’extension essentiels et des propriétés système requises pour Signature de code la fonctionnalité. **Le module d’extension Enterprise** affiche le module d’extension principal nécessaire aux opérations de signature.
Propriété d’adhésion	Champ de texte	Marqueur de configuration qui active les Signature de code options. **Remarque :** Ce paramètre doit être **Actif** pour confirmer que la signature de code fonctionne en fonction de l’exigence spécifique.
État de validation de la signature	Champ de texte	Indique si la validation de la signature est appliquée pendant l’exécution du code pour vérifier que seuls les scripts approuvés sont exécutés.
États des signatures	Graphique à secteurs	Vue d’ensemble complète de toutes les signatures de script, y compris leur état de validation actuel. Les signatures sont classées en : • **Les signatures approuvées** sont valides et associées à un certificat de signature de code approuvé. • **Les signatures non approuvées** échouent à la validation ou sont liées à un certificat de vérification non approuvé. • **Les signatures orphelines** sont présentes, mais ne sont plus liées à un certificat connu ou actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du tableau de bord (suite)

Titre	Type	Description
		Remarque : Utilisez ces informations pour évaluer l'intégrité du script et prendre des mesures correctives si nécessaire.
État de configuration du Serveur MID	Graphique à secteurs	État et relation de confiance de tous les MID Servers de votre instance. Utilisez cette section pour afficher le nombre total de MID Server et vérifier leur état. • **Serveurs MID actifs** : nombre de serveurs en cours d'exécution et connectés avec succès. • **Serveurs MID inactifs** : nombre de serveurs qui ne sont pas en cours d'exécution ou qui sont déconnectés.
Enregistrements signés par type	Graphique à secteurs	Distribution des enregistrements signés par type d'enregistrement, avec le pourcentage de couverture dans les catégories suivantes : • **Règles métier** : pourcentage d'enregistrements de règles métier signés. • **Includes de script** : pourcentage d'enregistrements d'include de script signés. • **Autres** : pourcentage d'enregistrements signés dans d'autres catégories prises en charge.
Enregistrements signés par application	Graphique à secteurs	Distribution des enregistrements signés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du tableau de bord (suite)

Titre	Type	Description
		entre différents modules d'application, indiquant le pourcentage de couverture de signature de code. • **Gestion des utilisateurs** : pourcentage d'enregistrements signés dans le module Gestion des utilisateurs. • **Validation du formulaire** : pourcentage d'enregistrements signés liés à la validation du formulaire. • **Autres** : pourcentage d'enregistrements signés dans tous les autres modules d'application.

Statut de vérification de signature

Affichez l'état des signatures valides, non valides et orphelines dans différentes applications pour évaluer la couverture de la signature de code. Utilisez ces informations pour identifier les domaines qui peuvent nécessiter une attention ou une action supplémentaire.

Le tableau de bord État de vérification de signature affiche les rapports suivants :

Tableau de bord de l'état de vérification de signature

Titre	Type	Description
Nom de script	Champ de texte	Identificateur ou titre affecté à un script spécifique dans le système.
Type	Champ de texte	Catégorie du script dans le système. Il aide à définir le rôle et la fonctionnalité du script. Exemple : • Business Rule • Include de script • Script client • Action de flux
Application	Champ de texte	Module ou zone du système dans lequel le script est appliqué. Exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de l'état de vérification de signature (suite)

Titre	Type	Description
		• Gestion des utilisateurs • Reporting • Validation du formulaire • Workflow • Notifications
Statut	Champ de texte	Indique l'état actuel de vérification de la signature du script. • **Valide** : la signature du script est vérifiée et approuvée. • **Non valide** : la signature du script n'est pas vérifiée ou est considérée comme non fiable.
Dernière analyse	Champ de texte	Date et heure auxquelles le script a été scanné pour la dernière fois pour la vérification de la signature au format : JJ/MM/AA/H (Jour/Mois/Année/Heure :Minute)

Signature de code Configuration de Serveur MID

Gérez et configurez les relations d'approbation et les paramètres de certificat pour les serveurs MID.

Le tableau de bord Configuration de Serveur MID de signature de code affiche les rapports suivants :

Signature de code Configuration de Serveur MID

Titre	Type	Description
Serveur MID	Champ de texte	Nom de l'instance de Serveur MID spécifique.
Statut	Champ de texte	État opérationnel actuel du Serveur MID. • **Actifs** • **Inactif**
Version	Champ de texte	Version logicielle du serveur MID actuellement utilisée. Utilisez ces informations pour :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signature de code Configuration de Serveur MID (suite)

Titre	Type	Description
		• Assurez-vous de la compatibilité avec votre instance. • Assurez-vous que le serveur exécute les dernières fonctionnalités prises en charge et mises à jour de sécurité.
Dernier enregistrement	Champ de texte	Date et heure les plus récentes auxquelles le Serveur MID a communiqué avec l'instance au format suivant : JJ/MM/AA/H (Jour/Mois/Année/Heure :Minute)

Paire de clés et certificats

Le tableau de bord Paires de clés et certificats affiche des détails sur les clés cryptographiques et les certificats numériques utilisés pour Signature de code. Elle comprend des informations telles que le type de clé, l'émetteur du certificat, la date d'expiration et l'état de validité. Utilisez ce tableau de bord pour gérer les informations d'identification de certificat de signature de code, vérifier leur validité et garantir des opérations sécurisées et fiables Signature de code .

Le tableau de bord Configuration de la paire de clés et des certificats affiche les rapports suivants :

Configuration de la paire de clés et des certificats

Titre	Type	Description
Nom du certificat	Champ de texte	Identificateur unique (nom) affecté à un certificat digital utilisé pour Signature de code.
Module de chiffrement	Champ de texte	Composant cryptographique utilisé pour générer, stocker et gérer les clés privées de Signature de code. Il garantit des opérations clés sécurisées et aide à protéger le matériel cryptographique sensible contre tout accès non autorisé.
Type	Champ de texte	Classification de la clé cryptographique ou du certificat utilisé pour Signature de code. Exemple : • ServiceNow • Tiers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la paire de clés et des certificats (suite)

Titre	Type	Description
Date d'expiration	Champ de texte	Date à laquelle le certificat digital expire et n'est plus valide.
Statut	Champ de texte	Validité actuelle du certificat numérique. • **Valide** : le certificat est actif et peut être utilisé pour Signature de code. • **Expiré** : le certificat a dépassé sa date d'expiration et n'est plus valide. • **Expiration prochaine** : la date d'expiration du certificat approche. Utilisez cet état pour prendre des mesures proactives de renouvellement afin d'éviter toute interruption des opérations de signature de code.
Chaîne	Champ de texte	La chaîne de certificats, qui comprend le certificat numérique ainsi que les certificats intermédiaires et racines qui établissent un chemin d'accès de confiance. Sélectionnez **Afficher la chaîne** pour afficher la chaîne de certificats.

Configuration de la signature de code

Le tableau de bord Configuration de la signature de code affiche les propriétés système et les paramètres clés qui contrôlent Signature de code votre environnement, y compris les marqueurs et les politiques d'application. Ces paramètres activent les fonctionnalités, appliquent la validation de signature et définissent des sources de confiance.

Le tableau de bord Configuration de la signature de code affiche les rapports suivants :

Configuration de la signature de code

Titre	Type	Description
Paramètre	Champ de texte	Nom d'une propriété de configuration spécifique qui contrôle une fonctionnalité ou un comportement lié à la signature de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la signature de code (suite)

Titre	Type	Description
		code. Chaque paramètre définit la façon dont le système doit gérer des aspects tels que la validation des signatures, l'application ou les sources de confiance.
Valeur	Champ de texte	État ou entrée actuelle affecté à un paramètre spécifique. Il détermine le comportement du paramètre. Par exemple, si est Signature de code activé (vrai) ou désactivé (faux). La valeur affecte directement les opérations et l'application Signature de code du système.
Dernière mise à jour	Champ de texte	Date et heure les plus récentes auxquelles le paramètre a été modifié au format suivant : JJ/MM/AA/H :S (Jour/Mois/Année/Heure :Minute)

Référence de signature de code

Les rubriques de référence fournissent des informations supplémentaires pour administrer et dépanner la signature de code.

Propriétés installées avec Signature de code

La signature de code ajoute les propriétés suivantes.

Dépannage et accès aux journaux

Accédez à différents journaux pour résoudre les problèmes et identifier les causes des défaillances.

Propriétés installées avec Signature de code

La signature de code ajoute les propriétés suivantes.

Propriété	Type	Description
com.glide.codesigning.expanded.tracking.enabled	true|false	Si la valeur est « vrai », la longueur de validation de la pile de métadonnées est augmentée pour ecc_queue rubriques répertoriées dans la propriété **com.glide.codesigning.expanded_tracking.topic.list** . **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.expanded.tracking.length	Entier	Niveaux de validation de signature de code à appliquer lorsque la signature de code est activée. La valeur par défaut est de 3.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
		Important : Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.expanded_tracking.rubrique.liste	Chaîne	Liste séparée par des virgules des rubriques à soumettre à un suivi accru de la pile méta. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.agent.validation.exclusion.list	Chaîne	Liste séparée par des virgules des agents de ecc_queue pour lesquels la signature de code doit être ignorée
com.glide.codesigning.tracking.debug	true|false	Si la valeur est vrai, la journalisation des débogages pour le suivi de signature de code est activée.
com.glide.codesigning.tracking.enabled	true|false	Si vrai, active le suivi de l'appelant de signature de code. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.logging.enabled	true|false	Si vrai, active la connexion pour le suivi de la signature de code.
com.glide.codesigning.tracking.unsupported_script_tracking.active	true|false	Si vrai, les enregistrements ecc_queue insérés via des scripts non pris en charge (si détecté) ne sont pas notarisés. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.validation.fail_fast	true|false	Si vrai, la vérification de la signature de code échoue au premier échec de validation du script au lieu de vérifier tous les scripts. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.event_handler.code_signing.tracking	Chaîne	Définit le gestionnaire d'événements qui permet de s'assurer que les clients qui viennent d'activer la signature de code sont configurés pour être aussi sécurisés que possible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
		Important : Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.web_service_outbound.impl.codesigning.tracking	true|false	Si vrai, active le suivi de signature de code SOAPMessageV2 **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
com.snc.csf.maximum_update_size	Entier	Nombre maximal d'enregistrements autorisés dans un ensemble de mises à jour de signature de code. Cette valeur doit être limitée à une valeur comprise entre 6000 et 10 000. Si cette valeur est dépassée, plusieurs ensembles de mises à jour sont générés et liés au même ensemble de mises à jour parent pour permettre le traitement par lots. Cette limitation empêche les problèmes d'interface utilisateur décrits dans KB0557104 .
com.snc.csf.servicenow_root_of_trust.désactivé	true|false	Indique si la fonctionnalité de racine de confiance est active. La valeur par défaut est `faux`, ce qui signifie que les ServiceNow certificats de version sont approuvés. **Important :** Cette propriété ne peut être modifiée qu'à l'aide d'une tâche planifiée signée par un utilisateur ayant les rôles d'administrateur, d'administrateur de sécurité et de gestionnaire KMF. Pour en savoir plus sur la modification de votre racine de confiance, reportez-vous à la section Modifier votre configuration de la racine de confiance.
com.snc.kmf.signature.validation.optin	true|false	Si la valeur est vrai, active la signature de code sur votre instance. **Important :** Cette propriété ne peut être modifiée que par le biais d'une demande adressée à Service client et assistance.
glide.jdbcprobeloader.tracking	true|false	Active ou désactive la signature de code pour les sources de données JDBC. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
glide.rest.codesigning.tracking	true|false	Si vrai, active le suivi de signature de code RESTMessageV2. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.

Rôles installés avec Signature de code

La signature de code comprend les rôles suivants.

Administrateur de signature de code [codesigning_admin]

Utilisez le rôle d'administrateur de signature de code pour affecter des rôles de codesigning_manager et de codesigning_auditor à d'autres utilisateurs.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

Gestionnaire de signature de code [codesigning_manager]

Utilisez le rôle de gestionnaire de signature de code pour créer et mettre à jour la configuration de signature, ainsi que pour créer et exécuter des tâches de signature de code.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Auditeur de signature de code [codesigning_auditor]

Utilisez le rôle d'auditeur de signature de code pour afficher les configurations de signature et les tâches de signature. Le rôle d'auditeur n'a pas d'accès de création ou d'écriture aux actifs de signature de code.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

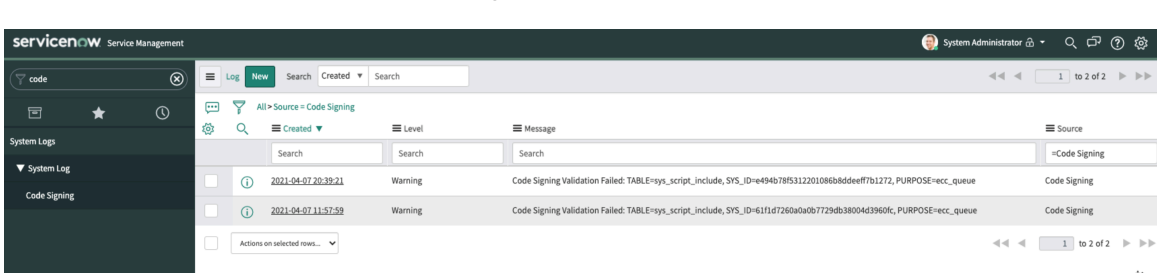
Aucun.

Dépannage et accès aux journaux

Accédez à différents journaux pour résoudre les problèmes et identifier les causes des défaillances.

Journaux de signature de code

Si l'un des enregistrements de file d'attente ECC n'est pas signé par l'API de suivi de signature de code, les messages non signés et les détails requis sont affichés dans le module Signature de code. Accédez à la **Journaux système** > **Journal système** > **Signature de code** pour accéder à la liste des enregistrements qui ne sont pas approuvés.



Pour les journaux de nœud de débogage supplémentaires, activez `com.glide.codesigning.tracking.debug` et définissez sa valeur sur `vrai`.

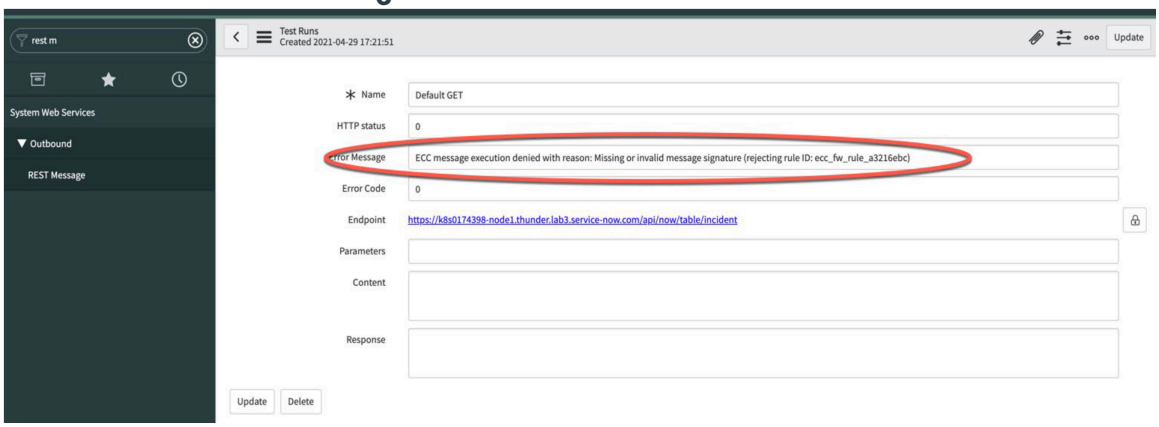
Échec de la validation de la signature du message REST sur Serveur MID

Accédez au message d'erreur relatif à l'échec de la validation de la signature en accédant à **Services web du système** > **Sortant** > **Message REST** et l'ouverture de l'enregistrement de message REST requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

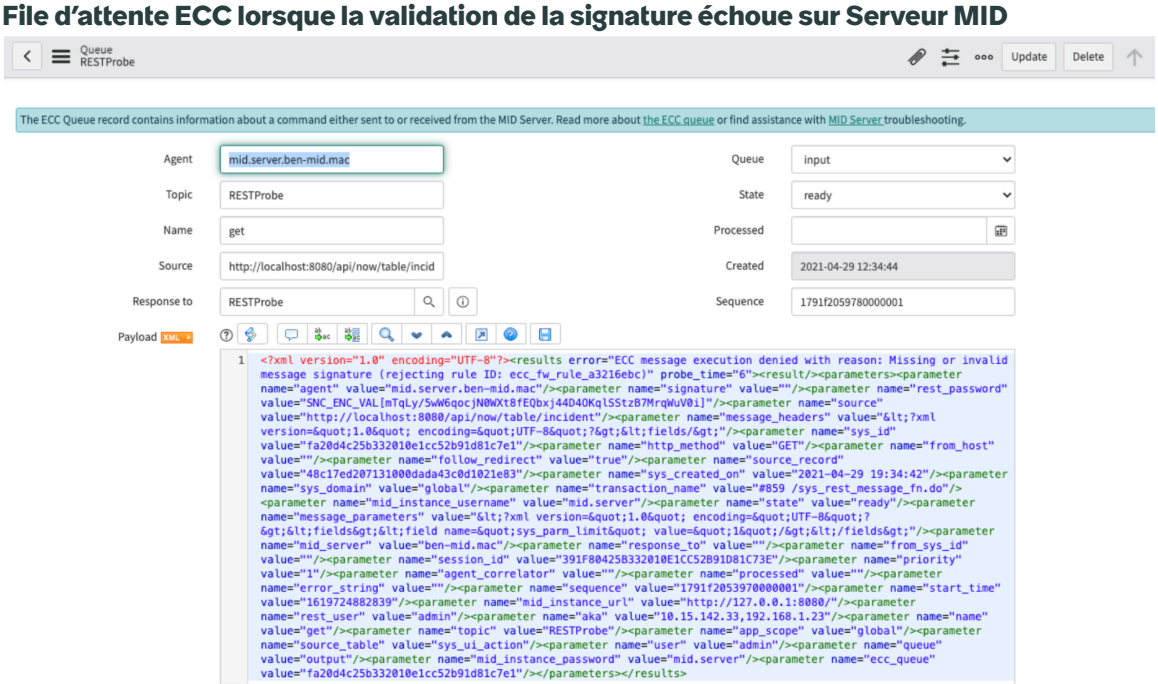
Échec de la validation de la signature sur Serveur MID



Remarque :

Les messages d'erreur associés aux rejets du pare-feu ECC commencent par Exécution du message ECC refusée.

File d'attente ECC lorsque la validation de la signature échoue sur Serveur MID



Message d'erreur lorsque le message ECC est bloqué par la règle d'utilisateur



Traduction automatique

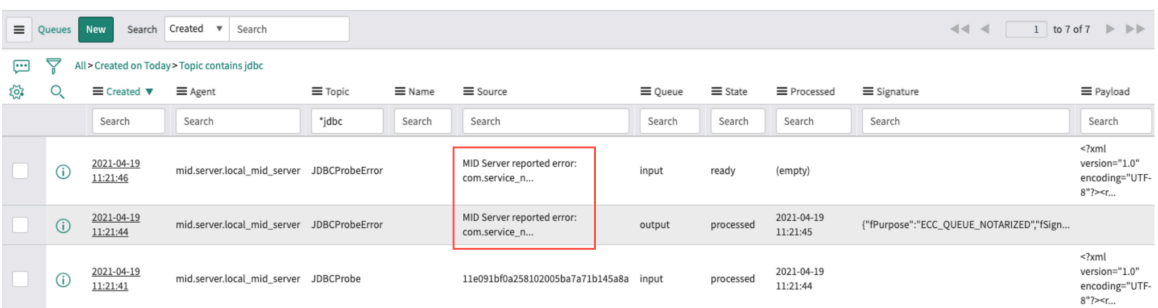
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sonde JDBC

Lorsqu'une source de données JDBC avec une signature non valide ou manquante est exécutée sur un Serveur MID, un message d'erreur avec les détails requis s'affiche.



La source affiche également les détails du message d'erreur.



Serveur MID Journaux

Pour activer la journalisation de pare-feu ECC détaillée, augmentez le niveau de journalisation en définissant la valeur du paramètre de configuration du serveur MID, `mid.log.level`, sur TRACE. Les journaux détaillés fournissent des informations sur :

- Règles chargées Serveur MID à partir du fichier de configuration de démarrage.
- Trace d'exécution granulaire des règles.
- Règle spécifique en vertu de laquelle un message ECC doit être accepté ou rejeté.

Remarque :
Si boot-config.xml n'est pas valide, les détails de l'échec Serveur MID au démarrage et de l'échec sont consignés dans les journaux de l'agent MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyse antivirus

Utilisez Analyse antivirus pour protéger votre instance contre les virus que les pièces jointes de fichiers peuvent introduire dans vos enregistrements système, notamment les incidents, les problèmes et les stories.

Explorer l’analyse antivirus



Découvrez la valeur de l’analyse antivirus.

Configurer la protection antivirus



Découvrez comment configurer la protection antivirus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résoudre les fichiers infectés



Découvrez ce qu'il faut faire avec les fichiers infectés.

Référence pour l'analyse antivirus



Connaître les attributs du dictionnaire pour l'analyse antivirus.

Traduction automatique

Exploration de l'analyse antivirus

Utilisez Analyse antivirus pour protéger votre instance contre les virus que les pièces jointes de fichiers peuvent introduire dans vos enregistrements système, notamment les incidents, les problèmes et les stories.

Analyse antivirus Analyse les pièces jointes stockées dans votre table de pièces jointes [sys_attachment] pour protéger les utilisateurs contre le chargement et le téléchargement de fichiers infectés. Tous les types de documents pris en charge par la plateforme sont analysés par l'analyse antivirus.

Si Analyse antivirus cette option est activée, toutes les pièces jointes de la table Pièces jointes [sys_attachment.do] sont analysées par défaut.

Le module d'extension Protection antivirus (com.glide.snap) est activé par défaut sur votre instance. En tant qu'administrateur, vous pouvez désactiver et réactiver la Analyse antivirus fonctionnalité sur votre instance en appuyant sur un bouton bascule, définir les options de configuration et examiner l'activité antivirus sur l'instance.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Analyse antivirus est également disponible pour les clients dans l'environnement GCC (Government Community Cloud) et commercial.

  Les utilisateurs GCC doivent définir la propriété (com.glide.snap.fed_enable_scan) sur vrai pour commencer à utiliser la fonctionnalité.

  Les utilisateurs commerciaux doivent définir la valeur `com.glide.snap.enable_scan` sur vrai.

- Les protocoles de communication HTTP et HTTPS sont pris en charge.
- Les fichiers chiffrés Edge sont exclus de cette analyse.
- Les définitions antivirus sont mises à jour tous les jours.
- Tout fichier de plus de 100 Mo n'est pas analysé.

Analyse des e-mails

Les e-mails entrants sont analysés à la recherche de virus par les filtres de messagerie système, et non par Analyse antivirus.

Champ Pièce jointe de fichier dans une table

L'ajout d'un champ **Pièce jointe** dans une table génère zz_yy tables. Ces tables sont dynamiques et virtuelles. Elles sont automatiquement générées lorsque **l'file_attachment** de type de colonne est ajoutée aux tables parentes.

Envisagez d'ajouter une photo de l'utilisateur à la table Utilisateurs et de l'incorporer dans la vue de formulaire. Lorsqu'une photo est téléchargée dans un enregistrement, la pièce jointe est automatiquement téléchargée dans la table sys_attachment. La table sys_attachment mappe la photo à la table zz_yyUsers.

Par défaut, seules les pièces jointes jointes à zz_yylive_profile tables sont analysées. Pour analyser d'autres tables de type colonne **, file_attachment** créer la propriété `com.glide.snap.scan.zz_yytables` système et insérer le nom de la table.

Exemple

Les tables « zz_yyincident » et « zz_yycase » sont des tables dynamiques créées lorsque la colonne est ajoutée aux tables parentes : Incident et Ticket, la valeur de la propriété doit être `zz_yyincident,zz_yycase`.

Une fois cette propriété définie, les pièces jointes pour les tables zz_yyincident et zz_yycase sont analysées.

Scénarios d'analyse

Examinez ces scénarios de chargement et de téléchargement pour comprendre comment le système identifie les menaces de sécurité potentielles à partir des fichiers joints à vos enregistrements.

Scénario 1 : charger un fichier

1. L'utilisateur télécharge sans le savoir un fichier infecté dans un enregistrement.
2. Le système analyse le fichier et le place en quarantaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Le fichier apparaît dans la fenêtre Pièces jointes, où il est marqué comme indisponible.
4. L'utilisateur sélectionne le fichier et ce message d'erreur s'affiche : Le fichier Infected_testing.txt n'a pas réussi l'analyse de sécurité. Veuillez supprimer le fichier de la INC0000059 d'enregistrement et réessayer.
5. Le système envoie une notification par e-mail à l'utilisateur et à l'administrateur antivirus.
6. L'utilisateur ferme la fenêtre Pièces jointes et revient à l'enregistrement. Le fichier infecté est affiché dans l'en-tête comme indisponible. Exemple : infected_testing123.txtZ [non disponible].

Scénario 2 - Télécharger un fichier

1. L'utilisateur ouvre un enregistrement pour télécharger un fichier qui lui est joint.
2. Ignorant que le fichier est infecté, l'utilisateur le sélectionne pour le télécharger.
3. Le système analyse le fichier, le place en quarantaine et affiche un message similaire à Le fichier infected_testing123.txt n'a pas réussi l'analyse de sécurité et ne peut pas être téléchargé.
4. L'utilisateur ferme le message et l'écran s'actualise, indiquant que le fichier n'est pas disponible.
5. Le système envoie une notification par e-mail à l'utilisateur et à l'administrateur antivirus.

Scénario 3 : télécharger un fichier ZIP

1. Un utilisateur ouvre un enregistrement et télécharge un fichier ZIP qui lui est joint.
2. Le système analyse les fichiers ZIP individuellement.
3. Un fichier ne passe pas l'analyse de sécurité et est marqué comme non disponible. Les fichiers restants sont compressés et téléchargés avec succès.
4. L'utilisateur ouvre le fichier ZIP et voit un fichier « error.txt » en plus du fichier téléchargé avec succès. Ce fichier contient un message d'erreur spécifiant quel fichier n'a pas passé l'analyse et n'a donc pas été inclus dans le ZIP.
5. L'utilisateur ouvre à nouveau l'enregistrement et voit que le fichier non disponible a été déplacé dans la section **Risques de sécurité potentiels** de la fenêtre Pièces jointes et ne peut pas être téléchargé.

Traduction automatique

Configurer Analyse antivirus

Configurez Analyse antivirus sur l'ensemble de votre instance et au niveau de la table.

Avant de commencer

Rôle requis : antivirus_admin ou admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Analyse antivirus est actif par défaut dans votre instance, où il analyse automatiquement les pièces jointes pour identifier les fichiers infectés par des virus. Configurez la fonctionnalité en vous assurant que l'analyse est activée dans votre instance et en identifiant toutes les tables que vous souhaitez exclure de l'analyse.

Procédure
1. Accédez à la **Tous** > **Antivirus** > **Configuration**.
2. Lors de la configuration de la fonctionnalité, tenez compte des points suivants.
3. Sélectionnez **Enregistrer**.
4. Excluez des tables de l'analyse antivirus en les ajoutant à la **liste des tables exclues**.
   a. Accéder à la **définition du système** # **au dictionnaire**
   b. Recherchez la table que vous souhaitez exclure de l'analyse et sélectionnez la table dont le type est défini sur collection.
   c. Dans l'onglet **Attributs** , sélectionnez **Nouveau**.
   d. Ajoutez `Exclude_from_antivirus_scan` dans le champ Attributs et saisissez `Vrai` dans le champ **Valeur** .
   e. Sélectionnez **Soumettre**.

Résultats
Analyse antivirus est activé dans votre instance et la **liste des tables exclues** sur la page Configuration antivirus est remplie avec toutes les tables que vous avez exclues de l'analyse.

Examen des fichiers en quarantaine

Examinez les pièces jointes en quarantaine et prenez des mesures supplémentaires si nécessaire.

Avant de commencer
Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche
Surveillez vos entrées de fichiers en quarantaine sur la page Quarantaine antivirus à intervalles réguliers pour effectuer l'une des actions suivantes.

Procédure
1. Accédez à la **Tous** > **Antivirus** > **Quarantaine**.
2. Cochez la case en regard de chaque entrée mise en quarantaine sur laquelle vous souhaitez effectuer une action disponible.
3. Sélectionnez la liste déroulante **Actions sur les lignes sélectionnées** dans la bannière pour choisir l'action à effectuer sur la ligne sélectionnée entrée mise en quarantaine.

Résultats
Le système demande une confirmation et effectue l'action sélectionnée en fonction de votre entrée.

Information associée

Centre de sécurité de l'instance

Mesures antivirus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Examiner l'activité antivirus

Consultez le journal des activités antivirus qui suit toutes les activités qui se produisent sur les fichiers potentiellement infectés à partir du moment où ils sont découverts et placés en quarantaine.

Avant de commencer

Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche

Ce journal fonctionne comme un rapport qui capture l'activité antivirus, telle que la découverte, la suppression et d'autres événements possibles de fichiers mis en quarantaine.

Procédure

1. Accédez à la **Tous** > **Antivirus** > **Activité**.
2. Examinez le journal des fichiers mis en quarantaine.
   Vous pouvez afficher les actions effectuées dans la colonne Événement pour chaque fichier mis en quarantaine.

Que faire ensuite

Déterminez les enregistrements que vous souhaitez supprimer, restaurer, télécharger ou conserver dans le journal. Voir Examiner les fichiers en quarantaine

Présentation des attributs du dictionnaire pour Analyse antivirus

Les attributs du dictionnaire modifient le comportement de la table ou de l'élément décrit par l'enregistrement du dictionnaire. En tant qu'administrateur, vous pouvez définir les valeurs des attributs de dictionnaire pour modifier le comportement de la configuration d'Analyse anti-virus par défaut.

Attributs de dictionnaire pour Analyse antivirus

Nom	Valeur	Élément cible	Description
Exclude_from_antivirus_scan	vrai/faux	n'importe quelle table	Si vrai, les pièces jointes de la table sont exclues de l'analyse antivirus. Reportez-vous à la rubrique Configurer Analyse antivirus.
Supress_antivirus_email_notification	vrai/faux	n'importe quelle table	Si vrai, arrête l'envoi de notifications par e-mail générées par la plateforme lorsqu'un fichier potentiellement infecté est identifié.
Suppress_antivirus_ui_notification	vrai/faux	n'importe quelle table	Si vrai, arrête les notifications d'interface utilisateur générées par la plateforme lorsqu'un fichier potentiellement infecté est identifié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Altering tables and fields using dictionary attributes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assainisseur HTML

Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

Découvrir l’assainisseur HTML



Découvrez comment fonctionne l’assainisseur HTML.

Configurer l’assainisseur HTML



Configurez l’assainisseur HTML.

Activer l’assainisseur HTML



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrez comment activer l’assainisseur HTML.

Explorer l’assainisseur HTML

Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

Utilisez l’assainissement HTML pour vous assurer que le contenu HTML de votre instance ne contient pas de contenu potentiellement dangereux. L’assainissement HTML consiste à supprimer les balises HTML qui pourraient être utilisées pour compromettre votre instance, telles que `<![CDATA[<script>]]>`, `<link>`ou `<embed>` les balises qui peuvent être utilisées pour exécuter des scripts indésirables sur votre instance ou diriger vos utilisateurs vers du contenu indésirable. Les balises sûres qui contrôlent la mise en forme de votre contenu sont conservées. En tant qu’administrateur, vous pouvez personnaliser le contenu supprimé ou conservé. Vous pouvez également contrôler si l’assainissement s’applique à tout le contenu ou uniquement aux champs que vous spécifiez.

L’assainisseur HTML fonctionne en vérifiant la liste d’inclusion intégrée pour le balisage que vous souhaitez toujours conserver. L’assainisseur fournit l’include `de script HTMLSanitizerConfig` que les administrateurs peuvent utiliser pour modifier la liste d’inclusion intégrée. Des éléments peuvent également être ajoutés à la liste d’exclusion pour supprimer le balisage HTML. Le contenu de la liste d’exclusion remplace la liste d’inclusion.

Les types d’éléments suivants peuvent être ajoutés aux listes d’inclusion et d’exclusion :

- Attributs globaux
- N’importe quel élément HTML

Remarque :
Par défaut, les attributs d’URL tels que `href` et `src` ne prennent en charge que ces protocoles :

- `http`
- `https`
- `mailto`
- `données`

Par exemple :

```
<a href="https://community.servicenow.com/community">ServiceNow Community</a>
```

Remarque :
Pour en savoir plus sur la propriété qui contrôle l’utilisation `glide.html.sanitize_all_fields` de l’assainisseur HTML, consultez Activer l’assainisseur HTML [mis à jour dans Centre de sécurité 1.3] Paramètres de renforcement de la sécurité de l’instance.

Configurer urlAttributes et les protocoles

Vous pouvez configurer les urlAttributes et leurs protocoles dans l’include de script **HTMLSanitizer** . Par exemple :

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        - -
        - -
    }
```

Étant donné que `les notes` se trouvent dans la liste d'inclusion dans cet exemple, cette URL n'est pas nettoyée :

```
<a title="Lotus"
 href="Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257EE
A003456FD">Lotus</a></p>
```

Liste d'inclusion par défaut

Remarque :
La liste d'inclusion par défaut est une liste système et n'est pas accessible aux utilisateurs de l'instance.

```
BUILTIN_HTML_WHITELIST :{

   globalAttributes:{ attribute:["id","class","lang","title","style"],

                           attributeValuePattern:{}},

   label:{ attribute:["for"]},

   font:{ attribute:["color","face","size"]},

   a:{ attribute:["href","nohref","name","shape"]},

   img:{ attribute:["src","name","alt","border","hspace","vspace","align","height","width"},

   table:{ attribute:["border","cellpadding","cellspacing","bgcolor","background","align","no
 resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},

   tr:{ attribute:["background","height","width","align","valign","char off","char"]},

   thead:{attribute:["align","valign","char off","char"]},

   tbody:{attribute:["align","valign","char off","char"]},

   tfoot:{attribute:["align","valign","char off","char"]},

   colgroup:{attribute:["align","valign","char off","char","span","width"]},

   col:{attribute:["align","valign","char off","char","span","width"]},
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
p:{attribute:["align"]},

style:{attributeValuePattern:{"type":"text/css"}}

canvas:{ attribute:["height","width"]},

details:{ attribute:["open"]},

summary:{ attribute:["open","valign","char off","char"]},

button:{ attribute:["disabled","accesskey","type"]},

form:{},

input:{ attribute:["size","maxlength","checked","alt","src","type","disabled","readonly","accesskey","border","usemap"]},

select:{ attribute:["disabled","multiple","size"]},

textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},

option:{ attribute:["disabled","label","selected"]},

div:{ attribute:["align"]},

ol:{ attribute:["start","type","square"]},

ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},

li:{ attribute:["value","fb__id","itemprop"]},

span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},

br:{ attribute:["clear"]},

h3:{ attribute:["itemprop"]},

html:{ attribute:["xmlns","lang","xml:lang"]},

link:{ attribute:["rel","type","href","charset"]},

meta:{ attribute:["name","content","scheme","charset","http-equiv"]},

pre:{ attribute:["xml:space"]},

noscript:{},  h1:{},  h2:{},  h4:{},  h5:{},  h6:{},

i:{},  b:{},  u:{},  strong:{},  em:{},  small:{},  big:{},

pre:{},  code:{},  cite:{},  samp:{},  sub:{},  sup:{},

strike:{},  center:{},  blockquote:{},  hr:{},  map:{},

dd:{},  dt:{},  dl:{},  fieldset:{},  legend:{}, figure:{},  tt:{},
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
body:{},  caption:{},  head:{},  title:{},  shape:{},},
```

Utilisation de variables et de modèles dans les champs HTML

Les champs HTML/HTML traduits sont nettoyés HTML par défaut. Ce processus nettoie le code HTML d'entrée pour le protéger contre le script de site à site (XSS) et les attaques de sécurité associées. Stocker des modèles ou des variables telles que ${description} ou {{description}} ou similaire et les remplacer par une description vraie après le nettoyage réduira l'efficacité du processus de nettoyage. Cela est dû au fait que l'assainissement est appelé uniquement sur le modèle d'espace réservé et non sur le contenu HTML. Le stockage uniquement du contenu HTML dans les champs HTML/HTML traduit permet de garantir un processus de nettoyage efficace.

Configuration de l'assainisseur HTML

Vous devez modifier un include de script pour apporter des changements de configuration à l'assainisseur HTML.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Includes de script**.
2. Ouvrez **HTMLSanitizerConfig**.
3. Pour ajouter des éléments à la liste d'exclusion, utilisez la classe HTML_BLACKLIST.

   Pour ajouter des éléments à la liste d'inclusion, utilisez la classe HTML_WHITELIST.

   Utilisez ce format :

```
HTML_XXXXLIST :{
      globalAttributes :{

         attribute:[attribute-name1,...],
         attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}

      },<html-element-name>:{// Same as Above},----}
```

   - *`globalAttributes`* contient des éléments attribut ou attributeValuePattern qui s'appliquent globalement à tous les éléments HTML.
   - *`attribute`* est une liste d'attributs séparés par des virgules.
   - *`attributeValuePattern`* est un dictionnaire de paires attribut-valeur-regex-modèle. L'attribut-valeur-regex-pattern est une expression régulière qui doit correspondre à la valeur de l'attribut.

Example:
Prenons l'exemple suivant :

```
HTML_WHITELIST:{
      globalAttributes:{
         attribute:["id","name"],},
      img:{
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        attribute:["style","align"],
        attributeValuePattern:{src:".*jpeg"}},
    iframe:{},}
```

Il ajoute les éléments suivants à la liste d'inclusion :

- L'ID et le nom des attributs globaux. Il s'agit d'une liste de chaînes qui peuvent être appliquées globalement à tous les éléments.
- Élément img où les attributs sont stylisés et alignés.
- L'élément img dont l'attribut source de l'image est un fichier avec l'extension .jpeg. Ceci est un exemple de modèle d'expression régulière qui correspond à une valeur d'attribut.
- L'élément iframe.

Activation de l'assainisseur HTML

L'assainisseur HTML fournit une propriété permettant d'activer ou de désactiver l'assainisseur pour tous les champs HTML du système.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Par défaut, cette propriété est définie sur true pour les nouvelles instances.

Procédure

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Définissez les propriétés *`glide.html.sanitize_all_fields`* et *`glide.translated_html.sanitize_all_fields`* sur **vrai**.

> **Remarque :**
> Pour en savoir plus sur cette propriété, consultez Activer l'assainisseur HTML [mis à jour dans Centre de sécurité 1.3] Paramètres de renforcement de la sécurité de l'instance.

Trouble?

Si les propriétés n'existent pas dans la table Propriétés système, vous pouvez les ajouter.

Activer l'assainissement sur les champs individuels

Vous pouvez utiliser des attributs de champ pour activer ou désactiver l'assainisseur sur des champs individuels.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous devez d'abord définir la propriété assainisseur sur faux, puis activer l'assainisseur pour chaque champ pour n'importe quel formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la table sys_properties et définissez la valeur sur *glide.html.sanitize_all_fields* **faux**.
   Cela désactive l'assainisseur pour tous les champs HTML du système.
2. Accédez au formulaire qui contient le champ HTML.
3. Cliquez avec le bouton droit sur l'étiquette du champ HTML, puis sélectionnez **Configurer le dictionnaire**.
   Le formulaire Entrée du dictionnaire s'ouvre pour le champ HTML.
4. Entrez l'une des options suivantes dans le champ Attributs :
   - Pour désactiver le nettoyage, saisissez `html_sanitize=faux`
   - Pour activer l'assainissement, saisissez `html_sanitize=true`
5. Cliquez sur **Mettre à jour**.
6. Pour activer l'assainisseur HTML pour les champs HTML traduits, définissez la *glide.translated_html.sanitize_all_fields* propriété sur **vrai**.

Activer la connexion à l'assainisseur HTML

Lorsque l'assainisseur HTML supprime des éléments ou des attributs, ils sont ajoutés au journal système.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous pouvez consulter ces éléments expurgés en ajoutant /syslog_list.do ? sysparm_query=source %3DHTMLSanitizer à l'URL de votre instance.

Procédure

1. Pour examiner ces éléments expurgés , `ajoutez /syslog_list.do ? sysparm_query=source %3DHTMLSanitizer` à l'URL de votre instance.
2. Pour activer ou désactiver la journalisation, ajoutez la propriété `glide.html_sanitize.discarded_log.enable` aux propriétés système et définissez la valeur sur **vrai** (activé) ou **faux** (désactivé).
   Cette propriété est par défaut définie sur **true**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Audit

Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

Explorer



Découvrez les fonctionnalités et les valeurs commerciales de l’audit.

Configurer



Découvrez comment configurer l’audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue



Examinez les tables Sys Audit et Audit Relationship Change.

Référence



Connaître les ensembles d’historique.

Explorer l’audit

Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

Vue d’ensemble de l’audit

L’activation de l’audit suit la création, la mise à jour et la suppression de tous les enregistrements de la table. Si vous souhaitez auditer des champs individuels dans une table, vous pouvez masquer les champs que vous ne souhaitez pas suivre à l’aide d’un attribut de dictionnaire.

Les informations d’audit sont conservées dans les tables suivantes :

- Audit
- Connaître les ensembles d’historique

⚠ Avertissement :
L’audit des tables système qui reçoivent une quantité importante de trafic, telles que les contextes de workflow [wf_context] ou les alertes Gestion des événements [em_alert], peut avoir un impact sur les performances. Pour cette raison, vous ne pouvez pas auditer la table em_alert dans son ensemble. Au lieu de cela, auditez les domaines d’intérêt sélectionnés. À définir `audit=true` sur la table em_alert et sur les champs sélectionnés. Essayez d’auditer le moins de champs possible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Audit des utilisateurs

L'audit comporte les utilisateurs suivants.

- administrateur
- security_admin

Avantages de l'audit

Avantage	Fonctionnalité	Utilisateurs
Activer l'audit de table pour suivre les changements apportés à tout ou partie des champs de la table	Configuration de l'audit pour une table	administrateur
Découvrez une façon améliorée de définir et de configurer l'option d'audit	Configurer l'audit à l'aide de la console de gestion d'audit	administrateur
Automatiser et simplifier la suppression des données d'audit	Configurer votre rétention d'audit	security_admin

Ce qu'il faut explorer ensuite

Pour en savoir plus sur l'utilisation de l'audit, consultez :

- Configuration de l'audit pour une table
- Configurer l'audit à l'aide de la console de gestion d'audit
- Affichage des tables d'audit système et de changement de relation d'audit
- Connaître les ensembles d'historique

Audit des composants

Explorez les composants d'audit suivants pour mieux comprendre les tables d'audit, les suppressions et les exemptions.

Audit des tables parents et enfants

Les tables ne dérivent pas les marqueurs d'audit des tables auditées parentes ou enfants.

- Par exemple, si vous activez l'audit pour la table Éléments de configuration [cmdb_ci], seuls les CI stockés dans cette table de base sont audités.
- De même, si vous activez l'audit pour la table Ordinateurs [cmdb_ci_computer], seuls les enregistrements CI de l'ordinateur sont audités, y compris les champs de la table Ordinateurs [cmdb_ci_computer] dérivés de la table Éléments de configuration [cmdb_ci].

Audit des tables du système

Par défaut, le système n'audite pas la suppression d'un enregistrement des tables système. Pour auditer une table système, ajoutez-la à la liste des tables de la `glide.ui.audit_deleted_tables` liste des propriétés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Audit des suppressions à partir d'un formulaire ou d'une liste

Par défaut, le système vérifie les suppressions d'enregistrements individuels à partir d'un formulaire. Pour empêcher l'audit, définissez l'attribut `no_audit_delete`dictionnaire de la table .

Le système audite les suppressions d'une liste **lorsqu'il est** sélectionné dans le dictionnaire de table et que la table n'est pas répertoriée dans la `glide.db.audit.ignore.delete` propriété.

Remarque :
Par défaut, la `glide.db.audit.ignore.delete` propriété ne figure pas dans la table Propriétés système [sys_properties]. Pour modifier la propriété et ses valeurs associées, vous devez d'abord l'ajouter manuellement. Cependant, lorsqu'il est ajouté manuellement, il remplace les valeurs par défaut suivantes :

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_user_preference,sys_aud
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

Pour en savoir plus sur l'ajout de propriétés système, consultez Ajouter une propriété système

Il convient de noter que, par défaut, les suppressions d'audit sont activées, que l'enregistrement soit supprimé de la vue de formulaire, de la vue de liste ou via un script/ une tâche planifiée.

Informations auditées

L'audit suit les changements d'enregistrement suivants :

- L'identificateur d'enregistrement unique (sys_id) de l'enregistrement qui a changé
- Champ qui a changé
- Nouvelle valeur du champ
- Ancienne valeur du champ
- Nombre de fois où cet enregistrement et ce champ ont été mis à jour
- Date et heure auxquelles le changement s'est produit
- Utilisateur ayant effectué le changement
- Motif du changement (le cas échéant, motif associé au changement)
- ID de point de contrôle interne pour l'enregistrement, si l'enregistrement a plusieurs versions.

Informations exemptées d'audit

Certaines mises à jour ne sont pas auditées malgré l'activation de l'audit sur une table. Par exemple, vous pouvez voir 132 mises à jour dans l'historique d'un enregistrement, mais seulement sept mises à jour auditées.

L'audit exclut les informations suivantes :

- Mises à jour effectuées par une mise à niveau.
- Les mises à jour sont effectuées via des jeux d'importation.
- Enregistrements dans les tables parentes ou enfants.
- Champs avec l'attribut no_audit dictionnaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les tables système ne sont pas répertoriées dans la liste des `glide.ui.audit_deleted_tables` propriétés.
- Champs commençant par le préfixe sys_ (champs système), à l'exception des colonnes sys_class_name et sys_domain_id.
- Les pages de l'interface utilisateur peuvent parfois déclencher des mises à jour d'un enregistrement sans créer de journal d'audit.
- Chaque fois qu'un moniteur d'inactivité touche un enregistrement. Cela vous évite de voir des centaines de mises à jour répertoriées contre un incident, le bruit noyant les données utiles.
- Modifications manuelles des Analyse des performances scores.
- Application de l'ensemble de mises à jour
- Importer XML

Audit d'une table

Pour obtenir des instructions sur l'audit d'une table, reportez-vous à la section Configuration de l'audit pour une table.

Par défaut, le système suit tous les champs d'une table auditée. Vous pouvez auditer un sous-ensemble de champs dans une table de deux manières :

- Vous pouvez activer l'audit pour l'ensemble de la table, puis exclure les champs que vous ne souhaitez pas inclure. Elle est appropriée lorsque vous souhaitez auditer la plupart des champs, mais pas tous, et est appelée *liste d'exclusion*. Pour plus d'informations, consultez Exclure un champ de l'audit (liste d'exclusion).
- Vous pouvez activer l'audit pour la table, mais uniquement pour les champs spécifiés. Elle est appropriée lorsque vous souhaitez auditer uniquement un petit nombre de champs de la table et est appelée *liste d'inclusion*. Pour en savoir plus sur l'inclusion d'un champ à l'aide d'une liste d'inclusion, reportez-vous à la section Inclure un champ de table dans l'audit (liste d'inclusion).

Enregistrements d'audit non annulables

Réduisez les chances que les enregistrements d'audit ne soient pas enregistrés lorsqu'une transaction est annulée avec le nouveau paramètre par défaut.

Des audits ont été définis pour créer un enregistrement immédiatement dans la même transaction avec les opérations d'écriture d'enregistrement cible. Si l'enregistrement cible est supprimé, l'audit est toujours créé et conservé dans le module **NCA Test Audit Delete** .

Remarque :
Le processus d'audit amélioré est activé par défaut. Si la propriété glide.db.audit.lazy est définie sur True, le processus d'audit amélioré est désactivé.

Avant la Yokohama publication, si une transaction est annulée, certaines opérations auditables n'étaient pas enregistrées. Cela est dû au fait que la plateforme exécute certaines opérations entre le changement d'enregistrement et est annulée avant la création de l'audit. Mais désormais, les audits sont créés immédiatement après la modification de l'enregistrement, ce qui réduit les risques d'abandon de l'opération par une transaction annulée avant l'enregistrement de l'audit.

Les audits sont maintenant enregistrés dans le même thread que la transaction. Les audits précédents ont été créés dans un thread d'arrière-plan. Ce changement redéfinit la valeur par défaut de la propriété glide.db.audit.lazy de Vrai à Faux. Cette propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

n’est généralement pas définie dans la table Propriétés, car la majorité des instances commencent à utiliser la nouvelle valeur et le nouveau comportement par défaut. Sur certaines instances, cette propriété peut être déjà présente et définie sur Vrai, ce qui signifie que ces instances ne pourront pas utiliser ce changement pour auditer le comportement.

Remarque :
Il est recommandé de supprimer cette propriété pour tirer parti de la mise à jour.

Configuration de l’audit pour une table

Vous pouvez activer l’audit de table pour suivre les changements apportés à tout ou partie des champs de la table.

Avant de commencer

Remarque :
Les champs chiffrés ne sont pas audités par conception. Ce comportement n’est pas configurable.

Rôle requis : admin.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Dictionnaire**.
   Le système affiche la liste des entrées du dictionnaire. La liste comprend une ligne pour chaque table ainsi qu’une ligne pour chaque colonne (champ) de la table.
2. Dans la liste des entrées de dictionnaire, recherchez la ligne correspondant à la table que vous souhaitez auditer, par exemple `cmdb_ci_computer`.
   Vous pouvez distinguer la ligne de la table elle-même de celle d’une colonne de la table en trouvant la ligne avec le nom de table correct, une entrée vide **pour le nom** de colonne et un **type** de **collection**.
3. Sélectionnez l'entrée de dictionnaire pour la table.
   Le système affiche le formulaire d'entrée du dictionnaire.
4. Cochez la case **Audit** .
5. Sélectionnez **Mettre à jour**.

Que faire ensuite

Si vous souhaitez auditer uniquement quelques champs de la table Activer l’audit de la liste d’inclusion pour une table. Si vous souhaitez auditer la plupart des champs, mais en exclure certains, reportez-vous à la section Exclure un champ de l’audit (liste d’exclusion).

Activer l’audit de la liste d’inclusion pour une table

Activez une table pour auditer uniquement les champs que vous désignez explicitement. Cela est utile lorsque vous souhaitez auditer uniquement un petit nombre de champs dans une table auditée.

Avant de commencer

La table doit être activée pour l’audit.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Dictionnaire**.
   Le système affiche la liste des entrées du dictionnaire. La liste comprend une ligne pour chaque table ainsi qu'une ligne pour chaque colonne (champ) de la table.
2. Si nécessaire, personnalisez la vue de liste pour afficher la colonne **Attributs** .
3. Dans la liste des entrées de dictionnaire, recherchez la ligne correspondant à la table que vous souhaitez auditer, par exemple `cmdb_ci_computer`.
   Vous pouvez distinguer la ligne de la table elle-même de celle d'une colonne de la table en trouvant la ligne avec le nom de table correct, une entrée vide pour Nom de colonne et un type de *`collection`*.
4. Dans le champ **Attributs** de cette ligne, saisissez *`audit_type=whitelist`*.

Que faire ensuite

Indiquez les champs que vous souhaitez auditer dans cette table.

Exclure un champ de l'audit (liste d'exclusion)

Empêchez le ServiceNow AI Platform de suivre un sous-ensemble de champs dans une table auditée en excluant ces champs d'un audit.

Avant de commencer

Pour exclure un champ d'une table de l'audit, vous devez d'abord activer l'audit pour cette table.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Ajoutez un ensemble de champs à une liste d'exclusion lorsque vous souhaitez auditer la plupart des champs d'une table auditable. Si vous ne souhaitez auditer que quelques champs, suivez plutôt la procédure de liste d'inclusion .

Remarque :
La désactivation de l'audit sur les champs basés sur le journal peut avoir un impact sur la fonctionnalité de fonctionnalités, telles que le formateur d'activité. Pour plus d'informations, consultez KB0743142 .

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Dictionnaire**.
2. Si nécessaire, personnalisez la vue de liste pour afficher la colonne **Attributs** .
3. Accédez à la ligne correspondant à la table et au champ (colonne) que vous souhaitez exclure de l'audit.
4. Dans la colonne **Attributs** de cette ligne, saisissez `no_audit`.

Inclure un champ de table dans l'audit (liste d'inclusion)

Suivez un sous-ensemble de champs dans une table auditée en ajoutant ces champs à une liste d'inclusion.

Avant de commencer

Pour ajouter des champs dans une table à une liste d'inclusion, vous devez d'abord avoir activé l'audit pour cette table et activé l'audit de la liste d'inclusion pour cette table.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Ajoutez un ensemble de champs à une liste d'inclusion lorsque vous souhaitez auditer uniquement un petit nombre de champs d'une table auditée. Si vous devez auditer la plupart des champs et n'en exclure que quelques-uns, suivez plutôt la procédure de liste d'exclusion .

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Dictionnaire**.
2. Si nécessaire, personnalisez la vue de liste pour inclure l'affichage de la colonne **Attributs** .
3. Accédez à la table et au champ (colonne) que vous souhaitez ajouter à la liste d'inclusion.
4. Dans le champ **Attributs** , saisissez `audit=true`.

Activer l'audit pour une table système

Les suppressions des tables avec un préfixe sys_ ne sont pas auditées par défaut. Pour suivre les suppressions dans ces tables, ajoutez le nom de la table à la `glide.ui.audit_deleted_tables` propriété. L'activation du module d'extension Restaurer les enregistrements supprimés ajoute plusieurs valeurs par défaut à cette propriété.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Propriétés de l'interface utilisateur**.
2. Localisez la **liste des tables système (commençant par « sys_ » séparées par des virgules) dont la propriété de suppression a été auditée** .
3. Ajoutez ou supprimez des noms de tables.
   Les noms de tables doivent être séparés par des virgules, sans espace.
4. Sélectionnez **Enregistrer**.

Remarque :
Pour plus d'informations sur l'audit, voir Présentation de la table d'audit sys.

Configurer l'audit à l'aide de la console de gestion d'audit

Utilisez le module Console de gestion d'audit pour expérimenter un moyen amélioré de définir et de configurer l'option d'audit au sein de votre instance.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Console de gestion de l'audit**.
   La liste de toutes les tables de votre instance s'affiche.

Remarque :
Par défaut, la liste des tables pour lesquelles l'audit est activé s'affiche.

Vous pouvez sélectionner l'onglet **Désactivé** pour afficher la liste des tables pour lesquelles l'audit est désactivé. Vous pouvez également sélectionner l'onglet Tout pour afficher toutes les tables de votre instance avec l'option Audit activée ou désactivée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez la table dans la liste pour laquelle vous souhaitez mettre à jour les configurations d'audit.
   La table avec ses colonnes respectives s'affiche. Vous pouvez également voir le nombre total de colonnes dans la table sélectionnée.

   Remarque :
   Les colonnes et **la rétention** sont les onglets qui apparaissent sur la table.

3. Modifiez le bouton bascule Audit selon que vous souhaitez activer ou désactiver l'audit pour la table sélectionnée.

   Remarque :
   Lorsque l'audit est activé dans une table, toutes les colonnes et tous les champs de la table sont activés par défaut.

4. **Facultatif :** Sélectionnez **Modifier l'état de l'audit** si vous ne souhaitez pas que toutes les colonnes soient activées dans une table activée pour l'audit.
   La fenêtre modale Sélectionner les colonnes à modifier s'affiche.
5. **Facultatif :** Désélectionnez les colonnes que vous ne souhaitez pas activer.
   Vous pouvez également ajouter n'importe quelle colonne en cochant la colonne de la liste Colonnes disponibles.
6. Sélectionnez **Enregistrer** pour enregistrer les dernières modifications.
   Sélectionnez **Tout effacer** pour supprimer toutes les colonnes activées. Reportez-vous à la section Configurer votre rétention d'audit pour en savoir plus sur la conservation des données d'audit.

Configurer votre rétention d'audit

Utilisez l'option Rétention pour automatiser et simplifier la suppression des données d'audit selon vos besoins.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Console de gestion de l'audit**.
2. Sélectionnez la table dans la liste pour laquelle vous souhaitez mettre à jour la politique de conservation.

   Remarque :
   Par défaut, vous accédez à l'onglet Colonnes à la fin de cette étape.

3. Sélectionnez l'onglet Rétention pour mettre à jour la politique de conservation des données d'audit de table sélectionnées.
   Un modal affichant l'option de conservation s'affiche.
4. Activez le bouton bascule Purger automatiquement les enregistrements d'audit.
5. Sélectionnez la durée dans le menu déroulant Durée.
   Sélectionnez **Oui** si vous souhaitez poursuivre avec la durée sélectionnée. Vous pouvez également sélectionner **Annuler** si vous souhaitez sélectionner une durée différente.

   Remarque :
   Les journaux plus anciens que la durée définie seront purgés et ne pourront pas être restaurés.

   Le modal Politique de rétention s'affiche pour confirmer la durée sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Enregistrer** pour mettre à jour la politique de conservation de la table sélectionnée.
7. **Facultatif :** Pour désactiver la suppression des enregistrements d'audit d'une table, désactivez le bouton bascule Purger automatiquement les enregistrements d'audit et sélectionnez **Enregistrer**.

Remarque :
Les enregistrements d'audit précédemment supprimés en raison de la durée de conservation sélectionnée sont définitivement indisponibles.

Affichage des tables d'audit système et de changement de relation d'audit

Le système suit ServiceNow AI Platform les insertions et les mises à jour des enregistrements audités dans les tables Audit système (sys_audit) et Changement de relation d'audit (sys_audit_relation).

Les ServiceNow AI Platform pistes des tables d'audit. Pour suivre les tables, cochez la case **Audit** dans l'enregistrement du dictionnaire pour définir la valeur sur vrai. Par défaut, il n'audite pas les enregistrements des tables système, telles que les tables Ensembles de mises à jour.

Remarque :
Pour éviter les problèmes de performances et les boucles infinies, le système ignore toute règle métier ou workflow déclenché par des insertions dans la table Audit système.

Colonnes de la table d'audit système

Accédez à la table Audit système sur votre instance en saisissant `sys_audit.list` dans le filtre de navigation.

Les colonnes suivantes apparaissent dans les enregistrements de table sys_audit :

Champ	Description
Nom de la table	Table à laquelle appartient l'enregistrement d'audit (par exemple, « `incident` »)
Nom de champ	Colonne de la table à laquelle appartient l'enregistrement d'audit (par exemple, « `assigned_to` »)
Clé de document	Sys_id (identifiant d'enregistrement unique) pour l'enregistrement d'origine associé à l'enregistrement d'audit.
Utilisateur	Nom de l'utilisateur qui a créé le changement. **Remarque :** Certains processus automatisés utilisent le système ou l'utilisateur invité pour appliquer et suivre les modifications apportées aux enregistrements. Pour plus d'informations, consultez Utilisateurs système et invités.
Valeur précédente	Ancienne valeur du changement de champ représenté par cet enregistrement de sys_audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• Champs de référence : valeur sys_id unique de l'enregistrement changé. • Champs de date et d'heure : valeur du temps universel coordonné (UTC) telle que stockée dans la base de données.
Nouvelle valeur	Nouvelle valeur du changement de champ représenté par cet enregistrement de sys_audit. • Champs de référence : valeur sys_id unique de l'enregistrement changé. • Champs de date et d'heure : valeur du temps universel coordonné (UTC) telle que stockée dans la base de données.

Fonctionnement de la table Changement de relation d'audit (sys_audit_relation)

La table Audit système [sys_audit] suit les changements apportés aux champs de référence dans les tables marquées pour l'audit. Cette activité comprend des entrées de champ de journal et des jeux d'historique. La table Changement de relation d'audit [sys_audit_relation] suit les changements de relation entre sys_audit enregistrements de table et les tables sources d'où proviennent les enregistrements audités. Il permet également de savoir quand un enregistrement a pu être supprimé.

-
- Chaque fois que vous auditez un enregistrement d'une table, une relation est créée entre les différentes tables d'origine et le magasin qui enregistre les données. Ces informations de relation sont enregistrées dans les tables sys_history_set, sys_history_line et sys_journal.
- Si vous supprimez un champ associé à un enregistrement de table audité, la table sys_audit_relation enregistre la suppression. En d'autres termes, chaque fois que vous modifiez un enregistrement audité, il supprime d'abord les éléments passés, puis crée une relation dans la table sys_audit_relation avec de nouveaux ID de document.

Connaître les ensembles d'historique

Le système génère automatiquement des enregistrements d'ensemble d'historiques selon les besoins à partir de la table Audit lorsqu'un utilisateur crée un enregistrement ou en affiche l'historique.

Si un enregistrement se trouve dans une table auditée, son ensemble d'historique est généré lorsque l'enregistrement est inséré ou lorsqu'un utilisateur consulte l'enregistrement.

Remarque :
N'utilisez pas d'ensembles d'historique pour générer des rapports.

Plusieurs champs d'informations sont captés dans l'enregistrement de l'ensemble d'historique, affiché dans la vue de liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'enregistrement de la vue de liste

Champ	Valeur d'entrée
ID	ID de document pour l'enregistrement dont l'historique est en cours d'enregistrement.
Table	Table auditée pour l'enregistrement dont l'historique est en cours d'enregistrement.
Heure de chargement	Durée nécessaire pour générer l'ensemble d'historique.

Champs d'enregistrement de l'historique d'audit

Champ	Valeur d'entrée
Étiquette	L'étiquette du champ qui a été modifié.
Ancien	Valeur antérieure au changement.
Nouveau	Valeur après le changement.
Type	Indique si l'entrée concerne un champ normal, un enregistrement d'e-mail ou un enregistrement de changement de relation.
Numéro de mise à jour	Nombre de modifications de ce champ. La valeur -1 indique quand l'enregistrement a été créé ou supprimé.
Heure de mise à jour	Date et heure du changement. **Remarque :** L'heure de mise à jour des lignes d'historique générées automatiquement ne correspond pas à l'heure de création ou de mise à jour d'un enregistrement dans une situation de traitement spécifique. Lorsque vous affichez un ensemble d'historique d'un enregistrement pour la première fois, un ensemble initial d'enregistrements de lignes d'historique est généré automatiquement. Étant donné que les changements de fichier dans une mise à niveau ne sont pas audités, cette incohérence de date se produit lorsque : • Vous affichez un historique défini après qu'un changement a été apporté à un enregistrement, mais • Avant qu'une autre modification ne lui soit apportée lors d'une prochaine mise à niveau.
Nom d'utilisateur	Nom de l'utilisateur qui a créé le changement.

Ensembles d'historique dans une vue de calendrier

Une fois que les ensembles d'historique sont actifs, le choix du menu contextuel Historique est rempli à l'aide des informations provenant de l'ensemble d'historique plutôt que de la table `sys_audit` . Du point de vue de l'utilisateur, les mêmes données historiques sont disponibles dans la même interface utilisateur, mais la façon dont les informations sont stockées est différente.

Étant donné que la vue Historique inclut une vue de calendrier, mais n'utilise pas l'interface de liste normale pour filtrer et interagir avec les enregistrements d'historique, elle permet :

- Recherche et filtrage des données historiques.
- Exportation des données historiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des ensembles d'historique

Il existe deux façons d'afficher l'ensemble d'historique, accessibles via l'action du menu contextuel **Historique**.

Différences entre les ensembles d'audit et d'historique

Les tables Audit [sys_audit], Ensembles d'historique [sys_history_set] et Historique [sys_history_line] stockent les mêmes données, mais elles servent des objectifs différents et gèrent les données différemment.

Table d'audit [sys_audit]

La table Audit [sys_audit] est l'endroit où le système stocke les informations historiques de tous les enregistrements. Ces enregistrements sont destinés à être conservés pour toujours afin que les administrateurs puissent toujours suivre l'historique des enregistrements audités. À mesure que le nombre d'enregistrements d'audit augmente au fil du temps, il devient plus inefficace d'interroger directement la table d'audit pour obtenir des informations historiques. Il est beaucoup plus efficace d'exécuter des requêtes uniquement sur les enregistrements de sous-ensembles plus petits pour lesquels vous souhaitez réellement afficher les informations historiques.

Ensemble d'historique [sys_history_set] table

La table Ensemble d'historiques [sys_history_set] identifie les enregistrements particuliers d'une table auditée qui contiennent des informations historiques. La table Historique [sys_history_line] stocke les changements réels apportés aux valeurs de champ.

- Le système génère automatiquement un ensemble d'historiques et des enregistrements d'historique selon les besoins à partir de la table Audit lorsqu'un utilisateur crée un enregistrement ou demande son historique.
- Plutôt que de contenir un historique complet de tous les changements dans le système, les enregistrements d'historique et d'historique ne contiennent qu'un sous-ensemble récent d'informations historiques pour les enregistrements où les utilisateurs ont créé ou demandé de telles informations.
- Outre les données d'audit, les ensembles d'historique incluent également les informations définies lors de l'insertion d'enregistrement, y compris les entrées de champ journal. Les entrées de champ journal que vous créez avant de créer un enregistrement sont traitées de la même manière que les entrées de journal créées au moment de la création de l'enregistrement. Ces entrées de journal apparaissent dans des jeux d'historique avec la même heure de création et créés par des données que l'enregistrement associé lui-même.

Le système limite l'ensemble d'historique et les enregistrements d'historique par :

- Demander au nettoyeur de table de supprimer les enregistrements de l'ensemble d'historique qui n'ont pas été mis à jour depuis 30 jours.
- Utilisation de la rotation de table pour alterner entre quatre tables d'historique tous les sept jours. Le système supprime les enregistrements d'historique de plus de 28 jours.

Si quelqu'un a besoin d'informations historiques à nouveau à une date ultérieure, le système peut les régénérer à partir de l'audit des enregistrements sources.

Une fois que le système a généré des enregistrements de l'ensemble d'historique, le choix du menu contextuel **Historique** utilise l'ensemble d'historique plutôt que les enregistrements d'audit. Du point de vue de l'utilisateur, les mêmes données historiques sont disponibles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans la même interface utilisateur, mais la façon dont les informations sont stockées est différente.

Contrôler l'accès à l'historique

Vous pouvez donner à un rôle l'accès à l'affichage de l'historique des audits en définissant une propriété système.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Système**.
2. Sélectionnez la `glide.history.role` propriété dans la table.
3. Dans , sélectionnez les rôles d'utilisateur auxquels vous souhaitez accéder à l'historique `List of roles (comma-separated) that can access the history of a record`.
4. Sélectionnez **Enregistrer**.

Résultats

Les modifications apportées à un champ sont omises si un utilisateur sans accès en lecture affiche l'historique d'un enregistrement.

Modifier le nombre d'entrées d'historique

Par défaut, l'historique affiche un maximum de 250 entrées d'historique, mais vous pouvez modifier cette valeur.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Système**.
2. Sélectionnez la propriété `glide.history.max_entries`.
3. Définissez la `Maximum number of field entries displayed in record history, default is 250` valeur avec un nouveau nombre maximal d'entrées à afficher.

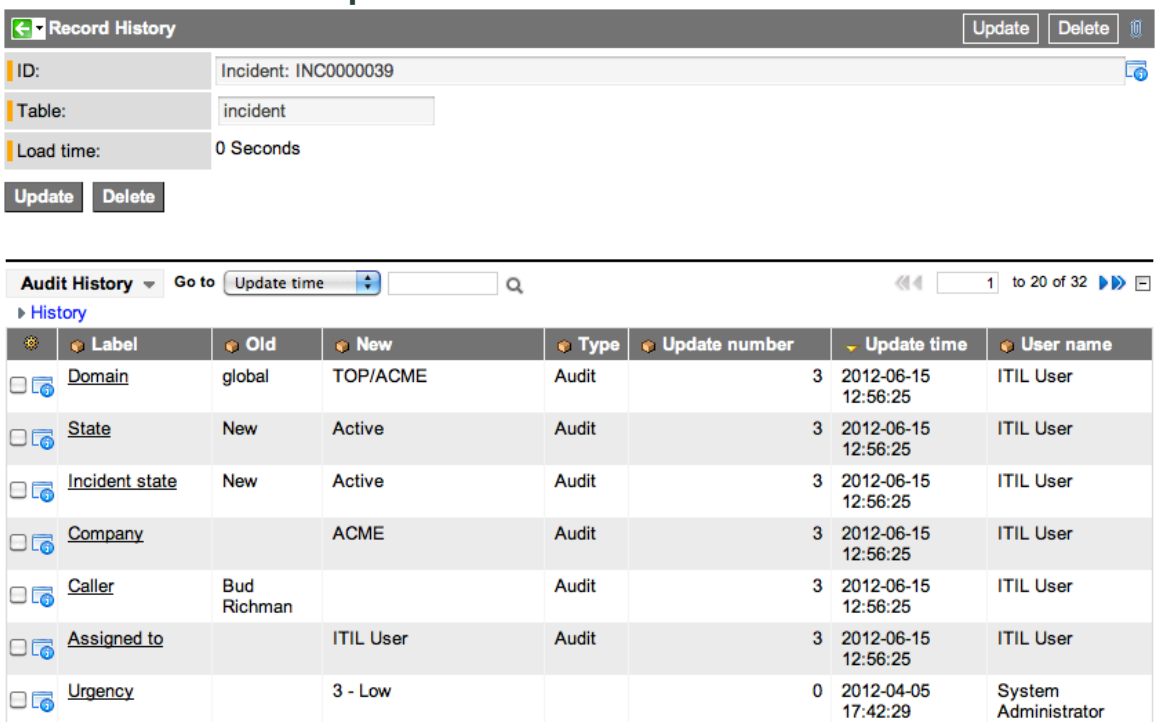
Liste de l'historique

La liste d'historique affiche chaque modification comme sa propre ligne dans la liste des modifications.

Traduction automatique

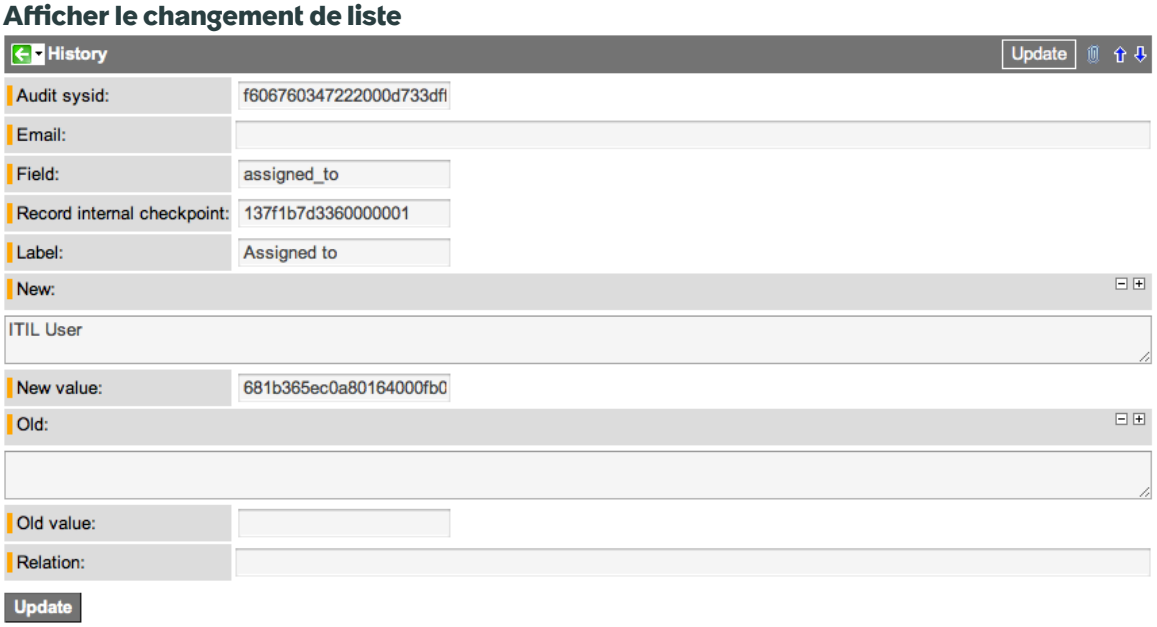
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher la liste de l'historique



Cliquez sur un élément de ligne pour afficher des détails supplémentaires sur le changement.

Afficher le changement de liste



Besoins

Pour afficher une liste d'historique, les conditions suivantes doivent être remplies.

Audit

L'audit de la table doit être activé pour afficher une liste d'historique.

ACL

Par défaut, l'option Historique de *liste* n'est disponible que pour les utilisateurs disposant du rôle d'utilisateur administrateur. Pour activer cette option pour les non-administrateurs, créez une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

règle ACL personnalisée accordant un accès en lecture à la table Historique des enregistrements [sys_history_set].

Rôles

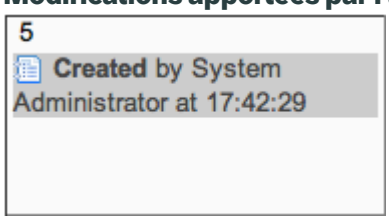
Au moins un des rôles dont dispose l'utilisateur doit être inclus dans la `glide.history.role` propriété, qui inclut le rôle itil par défaut.

Calendrier de l'historique

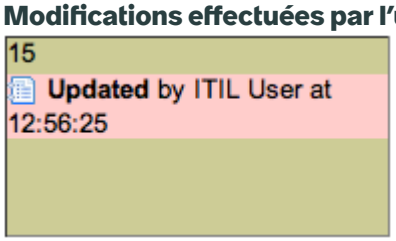
Le calendrier de l'historique indique les jours où l'enregistrement a été changé, la personne qui a effectué le changement et le moment où elle l'a effectué.

Le calendrier de l'historique est trié par numéro de mise à jour. Une couleur est affectée à chaque utilisateur afin que vous puissiez déterminer en un coup d'œil combien de fois un enregistrement a été modifié par un utilisateur spécifique. Par exemple :

Modifications apportées par l'administrateur système



Modifications effectuées par l'utilisateur ITIL

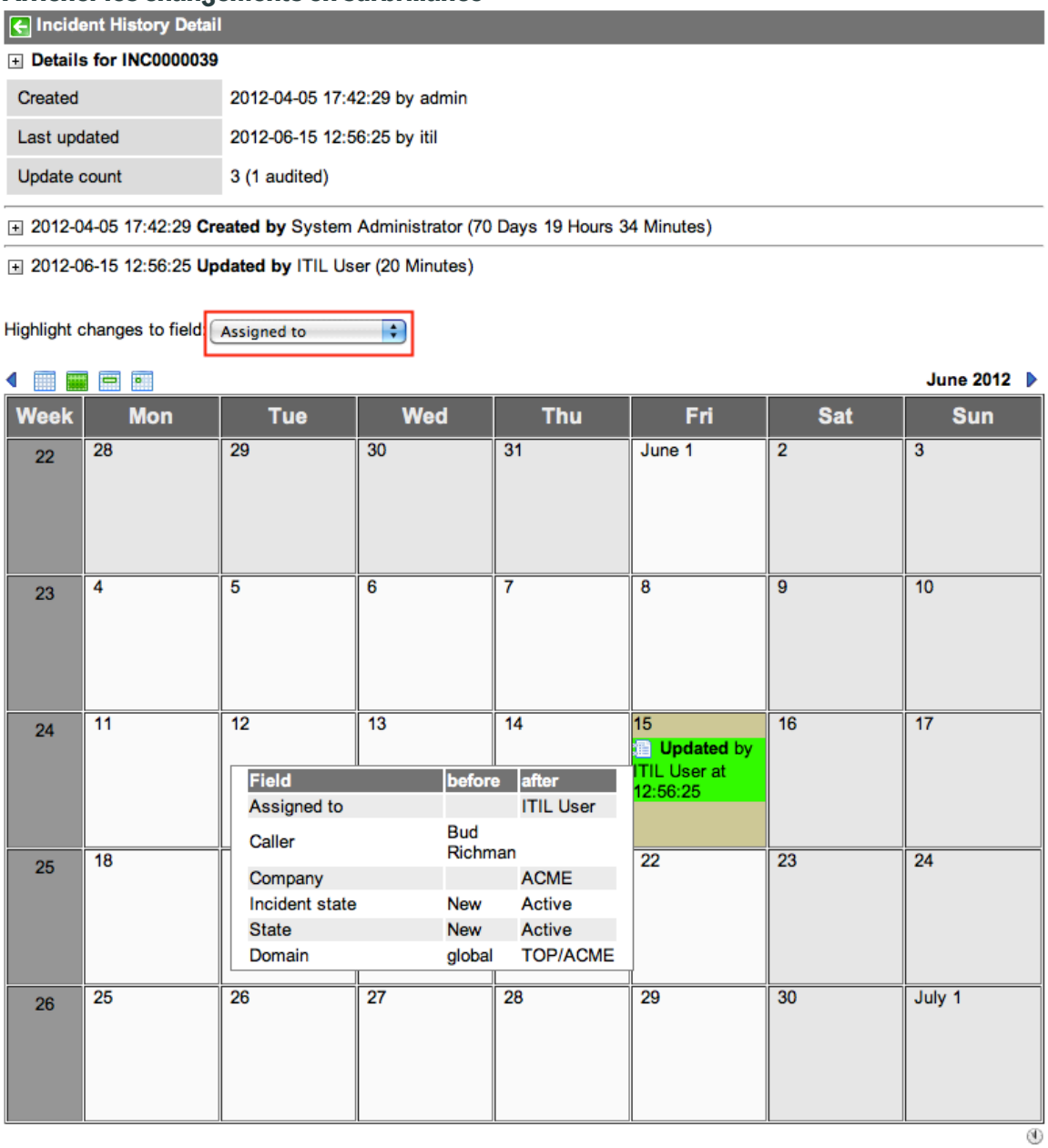


Pour mettre en évidence les changements apportés à un champ particulier, sélectionnez le champ dans la zone de sélection **Mettre en évidence les changements apportés au champ** . Le choix d'un champ dans cette zone de sélection modifie le calendrier pour mettre en évidence les heures auxquelles ce champ a été modifié. Passez la souris sur le texte de l'un des changements en surbrillance pour voir le changement de valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les changements en surbrillance

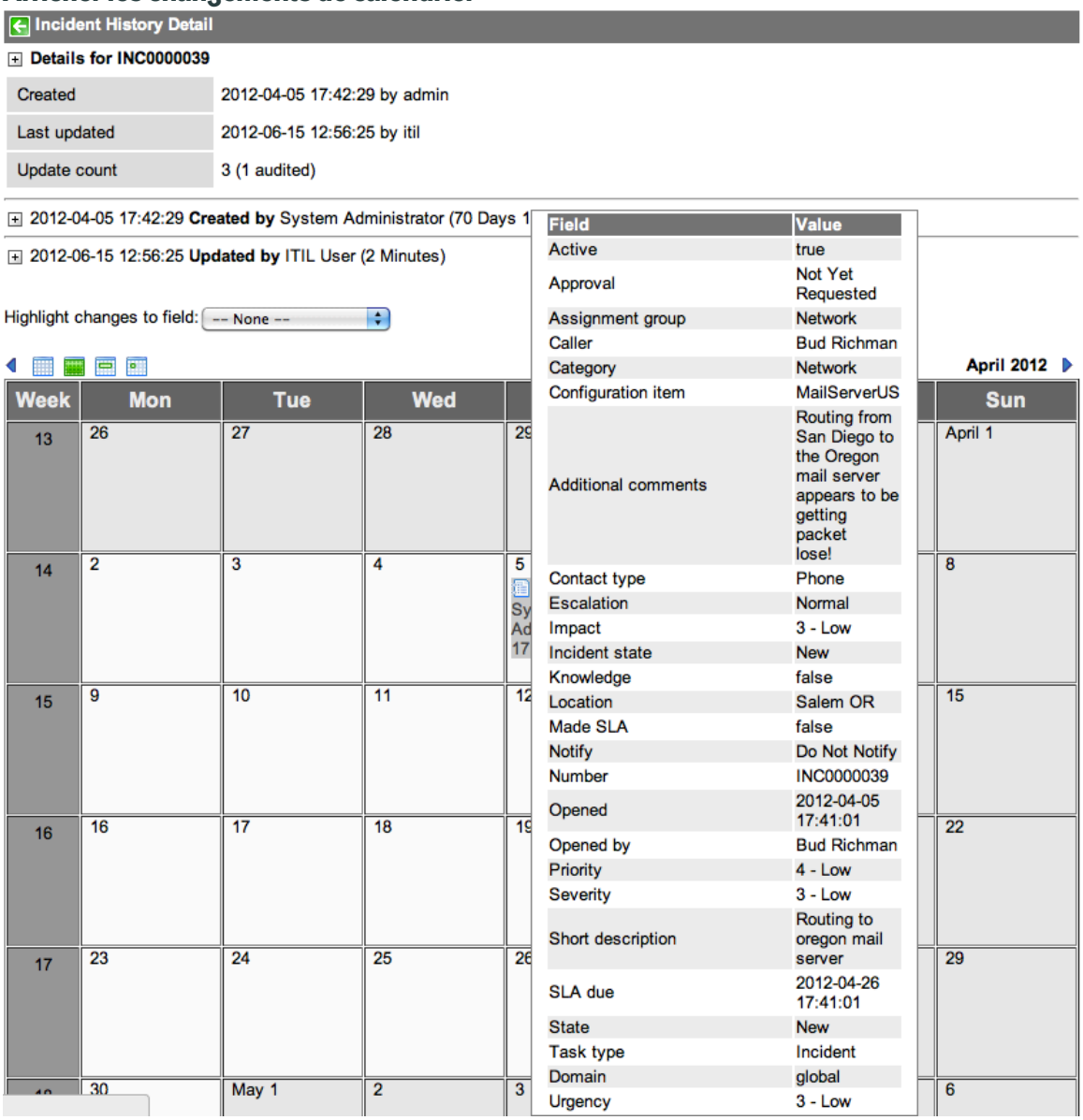


Si vous survolez l'icône dans une entrée, une fenêtre contextuelle affiche tous les changements de valeur. Il s'agit des mêmes informations que celles affichées dans la partie supérieure du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les changements de calendrier



Vous pouvez cliquer sur le numéro du jour pour obtenir une vue des changements pour ce jour. Vous pouvez également cliquer sur le numéro de semaine à gauche pour obtenir une vue de la semaine. Vous pouvez faire défiler d'un mois à l'autre pour voir les changements.

Chronologie de l'historique

Vous pouvez afficher une chronologie des changements pour un CI et pour ses enregistrements connexes, relations, bases de référence et changements proposés pour le CI. Les chronologies sont disponibles pour les CI dans la table Élément de configuration [cmdb_ci] ou un descendant de cette table, si l'audit est activé pour les tables.

Rôle requis : l'ACL de cette vue est basée sur les rôles définis dans la *glide.history.role* propriété système, qui est définie par défaut sur itil. En outre, l'utilisateur doit avoir un accès en lecture à la table Ensemble d'historiques [sys_history_set], qui est par défaut accordée à l'administrateur.

Vous pouvez ouvrir une chronologie lorsque vous affichez l'historique d'un CI. Vous pouvez spécifier la période, la plage horaire et les propriétés qui s'affichent dans la chronologie. Vous pouvez afficher ce qui a changé dans un ensemble de changements particulier ou

Traduction automatique

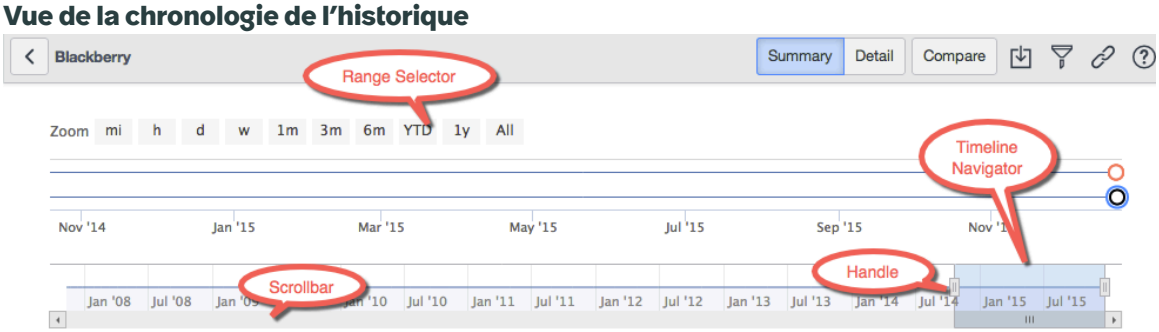
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

afficher l'intégralité du CI pour mieux résoudre les problèmes. Vous pouvez également afficher une chronologie des changements apportés aux enregistrements connexes du CI, et exporter et comparer des instantanés du CI à tout moment.

Les changements de CI sont représentés par des bulles de différentes formes et couleurs le long de la chronologie. La forme de chaque bulle représente un type de changement différent et la couleur de chaque bulle spécifie si le changement est valide ou non valide. Les bases de référence CI sont représentées par des cercles noirs que vous pouvez survoler pour afficher plus de détails. Cliquez sur l'icône **?** pour afficher les définitions de forme et de couleur des bulles, et pointez sur une bulle pour afficher les détails de l'ensemble de changements.

Un changement apporté à une relation n'est considéré comme valide que s'il a été appliqué via Gestion des changements. Si le changement a été appliqué via le cadre de travail des changements proposés, il est valide. Pour connaître les étapes de validation supplémentaires, reportez-vous à la section Créer ou modifier un script de validation planifiée .

Vue de la chronologie de l'historique



Bulles de chronologie



Remarque :
Les changements proposés qui n'ont pas de date de début planifiée sont placés à des moments futurs.

Navigateur de chronologie

Utilisez les poignées situées aux deux extrémités du navigateur de chronologie pour prolonger ou raccourcir la période affichée.

Vous pouvez faire défiler jusqu'à une autre période de temps en cliquant sur la partie inférieure du navigateur de chronologie, puis en faisant glisser le navigateur vers la gauche ou la droite.

Zoom

Par défaut, la chronologie du dernier mois s'affiche. En regard de l'étiquette **Zoom** au-dessus de la chronologie, vous pouvez sélectionner un autre intervalle de temps. Vous pouvez sélectionner des intervalles allant d'une minute à la période entière des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

S’il y a de nombreux changements du CI au cours de la période, les bulles affichées risquent d’être trop encombrées. Vous pouvez effectuer un zoom avant ou arrière pour répartir les bulles dans l’une ou l’autre des méthodes :

- Modifiez l’intervalle de temps dans la chronologie. Lorsque vous raccourcissez l’intervalle de temps, vous effectuez un zoom avant et lorsque vous allongez l’intervalle de temps, vous effectuez un zoom arrière.
- Sélectionnez la section de la chronologie sur laquelle vous souhaitez zoomer.

Filtre de propriété

Vous pouvez filtrer les bulles qui s’affichent. Par défaut, toutes les bulles sont affichées, représentant les changements apportés à toutes les propriétés du CI. Vous pouvez limiter la vue pour afficher uniquement les bulles dans lesquelles les propriétés sélectionnées ont changé et exclure les bulles dans lesquelles seules les propriétés non sélectionnées ont changé.

Les vues **Détails** et **Résumé** mettent en évidence les propriétés de votre périmètre de filtre qui ont changé. Les propriétés modifiées sont surlignées en bleu clair.

Dans la vue **Résumé** , vous pouvez choisir d’inclure toutes les propriétés du CI ou uniquement celles qui ont changé. Si vous choisissez d’afficher toutes les propriétés dans la vue récapitulative, les propriétés modifiées sont répertoriées avant les propriétés inchangées.

Vue de résumé

La vue **Résumé** affiche des instantanés des CI représentés par chaque bulle. Chaque instantané affiche les changements apportés aux champs et relations du CI en fonction de l’ensemble de changements. Il affiche les valeurs anciennes et nouvelles avant et après le changement, ainsi que toutes les relations qui ont été ajoutées ou supprimées.

Utilisez les boutons **>** et **<** des deux côtés de l’affichage de l’instantané pour parcourir les enregistrements d’ensemble de changements suivants et précédents dans un ordre chronologique.

Vue détaillée

La vue **détaillée** affiche les instantanés du CI qui correspondent aux bulles. Chaque instantané inclut les champs qui se trouvent dans le périmètre du filtre de propriété, affichant les propriétés qui ont changé sur un fond bleu clair. Cliquez sur une bulle pour afficher l’instantané correspondant du CI. Les données affichées sont en lecture seule.

Utilisez les boutons **>** et **<** des deux côtés pour parcourir les enregistrements d’ensembles de changements suivants et précédents dans un ordre chronologique.

Afficher la chronologie des changements apportés aux enregistrements connexes

Dans la chronologie des changements d’un enregistrement CI, vous pouvez également afficher une chronologie des changements pour les enregistrements connexes du CI.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Table cible : l'enregistrement du CI doit se trouver dans la table Élément de configuration [cmdb_ci] ou un descendant de cette table.
- Audit : doit être activé pour la table contenant le CI.

Procédure

1. Ouvrez la chronologie du CI.
2. Sélectionnez l'icône **Enregistrements connexes** et sélectionnez les enregistrements connexes dans la **liste des enregistrements connexes** à afficher.
   Cliquez à nouveau sur l'icône Enregistrements connexes pour afficher la chronologie des enregistrements connexes.

Résultats

La chronologie des changements apportés aux enregistrements connexes du CI s'affiche juste au-dessus de la chronologie du CI. Si vous décochez tous les enregistrements connexes, la chronologie des enregistrements connexes est masquée.

Que faire ensuite

Passez le curseur au-dessus d'une bulle de changement sur la chronologie des enregistrements connexes pour afficher les détails du changement, tels que la date et le nombre de propriétés modifiées. Lorsque vous modifiez l'intervalle de temps de mise au point, ou que vous effectuez un zoom avant ou arrière, cela affecte simultanément la chronologie des CI et la chronologie des enregistrements connexes.

Exporter un instantané d'un élément de configuration

Vous pouvez exporter un instantané d'un élément de configuration à partir de sa chronologie.

Avant de commencer

L'élément de configuration doit se trouver dans la table Élément de configuration [cmdb_ci] ou un descendant de cette table. L'audit doit être activé pour la table contenant le CI.
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter un instantané du CI au format XML, PDF (portail) ou PDF (paysage).

Procédure

1. Accédez à la **Tous** > **Configuration** > **Éléments de base** > **Tous** pour ouvrir la liste des éléments de configuration.
2. Ouvrez un enregistrement d'élément de configuration.
3. Ouvrez la chronologie de l'enregistrement.
4. Sélectionnez la bulle représentant la durée pendant laquelle vous souhaitez exporter un instantané du CI.
5. Cliquez sur l'icône d'exportation ( ).
6. Sélectionnez le format de fichier à utiliser pour l'exportation.
   Vous pouvez télécharger le fichier sur votre système pour consultation.

Comparer les instantanés de CI

Vous pouvez comparer les propriétés et les relations d'un CI à deux points différents de sa chronologie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Le CI doit se trouver dans la table Élément de configuration [cmdb_ci] ou un descendant de cette table. L'audit doit être activé pour la table contenant le CI.
Rôle requis : admin.

Procédure

1. Ouvrez la chronologie du CI.
2. Cliquez sur **Comparer**.
3. Sélectionnez une date de **début** et une date de **fin** .
4. Cliquez sur **Comparer**.

Suivi des changements apportés aux champs de référence

Les administrateurs peuvent suivre les changements apportés aux valeurs d'affichage des champs de référence.

Étant donné que les champs de référence ne stockent qu'une valeur d'ID, le système ne peut normalement auditer les changements que lorsque la valeur d'ID change. Par défaut, le système ne vérifie pas les changements lorsqu'une valeur d'affichage de champ de référence change.

Considérez la situation suivante. Un utilisateur change son nom de Jane Smith en Jane Miller. Étant donné que le nom d'utilisateur est la valeur d'affichage de la table Utilisateur, toute référence précédente à Jane Smith fait plutôt référence à Jane Miller. Si l'administrateur se contente de mettre à jour le nom de l'enregistrement utilisateur existant, les enregistrements d'audit et d'historique n'affichent que le nouveau nom Jane Miller. Par défaut, le système ne permet pas de distinguer les modifications apportées sous le nom d'utilisateur d'origine de celles apportées avec le nouveau nom d'utilisateur.

Si votre politique d'audit exige le suivi des changements de nom d'utilisateur, vous pouvez :

- Créez un nouvel enregistrement utilisateur pour le nouveau nom et désactivez l'enregistrement utilisateur précédent. Le système conserve les enregistrements d'audit pour l'ancien nom d'utilisateur et crée les enregistrements d'audit futurs avec le nouveau nom d'utilisateur.
- Créez des champs personnalisés et une règle métier pour enregistrer l'ancien nom et la date du changement de nom. Le système peut utiliser ces informations pour construire les noms appropriés dans les enregistrements d'audit et d'historique.

Insertions de suivi

Par défaut, le système ne crée pas d'enregistrements d'audit pour les insertions, car dans un cas classique, les insertions peuvent représenter plus de 80 % de la taille de la table d'audit.

Ne pas suivre les insertions permet d'obtenir de meilleures performances et une table d'audit beaucoup plus petite. Les administrateurs peuvent activer l'audit des insertions en définissant la `glide.sys.audit_inserts` propriété sur *vrai*.

Suivi des relations CI

Les changements apportés à une relation CI (Relations CI, Relations CI/utilisateurs ou Relations CI/groupe) apparaissent dans l'historique des éléments des deux côtés de la relation modifiée, que le changement soit manuel ou le résultat de Découverte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, si l'ordinateur alpha a une relation utilisé par le CI avec l'ordinateur bêta, alors l'historique de alpha a un enregistrement du moment où la relation avec bêta a été établie, et de même, l'historique de bêta a un enregistrement du moment où la relation avec alpha a été établie. Cet exemple illustre l'historique affiché lorsque des relations CI sont établies, puis que l'une des relations est supprimée :

Historique des relations CI

⊟ 2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

⊞ 2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

⊞ 2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

⊞ 2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

⊟ 2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

La puce Créé indique la date à laquelle le CI, l'utilisateur ou le groupe a été créé. La dernière puce d'activité fait référence à la date à laquelle les relations ont été modifiées pour la dernière fois. Si vous ne souhaitez pas afficher l'historique des relations CI pour un ou tous les types de relations CI, vous pouvez le désactiver en désactivant l'audit sur les tables de relations CI (Relation CI [cmdb_rel_ci], Type de relation CI/utilisateur [cmdb_rel_user_type] ou Relation de groupe [cmdb_rel_group]).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de sécurité élevée

Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.

Explorer le paramètre de haute sécurité



Découvrez les fonctionnalités et les valeurs commerciales des paramètres de sécurité élevée.

Activer les paramètres de sécurité élevée



Activez les paramètres de sécurité élevée.

Traduction automatique

Explorer les paramètres de haute sécurité

Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.

Le module Paramètres de sécurité élevée est activé avec le module d'extension Paramètres de sécurité élevée, qui est actif par défaut sur les nouvelles instances. Si les paramètres de sécurité élevée ne sont pas actifs sur votre instance, consultez Demande d'activation des paramètres de sécurité élevée. Pour en savoir plus sur ce module d'extension, consultez Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3] Paramètres de la sécurisation renforcée de la sécurité de l'instance. Les propriétés de ces types de paramètres de haute sécurité sont disponibles :

- Valeurs de propriété par défaut : pour renforcer la sécurité sur votre plateforme en centralisant tous les paramètres de sécurité critiques en un seul endroit pour la gestion et l'audit.
- Propriété de refus par défaut : fournit une propriété de gestionnaire de sécurité pour contrôler le comportement de sécurité par défaut pour l'accès aux tables.
- Rôle d'administrateur de sécurité : fournit un rôle permettant d'empêcher la modification des paramètres et ressources de sécurité clés. Le rôle d'administrateur de sécurité n'est pas hérité par le rôle d'administrateur et doit être explicitement attribué.
- Privilèges élevés : permet aux utilisateurs ayant le rôle d'administrateur de sécurité d'opérer dans le contexte d'un utilisateur normal et de s'élever à un rôle de sécurité plus élevé si nécessaire.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Contrôles d'accès aux propriétés : permet aux administrateurs de sécurité de définir les rôles requis pour lire et écrire les propriétés.
- Journaux système : sont en lecture seule.
- Règles de contrôle d'accès : contrôlez les données auxquelles les utilisateurs peuvent accéder et la façon dont ils peuvent y accéder.

Remarque :

- Les paramètres de sécurité élevée activent également automatiquement le module d'extension Sécurité contextuelle, s'il n'est pas déjà activé. En outre, Paramètres de sécurité de la plateforme : élevé fournit des paramètres et des fonctionnalités dans le contexte du renforcement de la sécurité de votre instance.
- Le contenu des paramètres de renforcement de la sécurité de l'instance contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le ServiceNow AI Platform.
- Pour en savoir plus sur chacune de ces propriétés, reportez-vous à la section Paramètres de sécurisation renforcée.

Il existe deux façons de définir ou de modifier les propriétés des paramètres de sécurité élevée.

- Accédez à la **Sécurité de système** > **Paramètres de sécurité élevée**.

  Les options de la page Propriétés de sécurité élevée sont **Oui** ou **Non**.

- Accédez à **sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **définies sur vrai** ou **faux**.

Contrôle d'accès à la propriété

Deux colonnes supplémentaires sont créées dans la table Propriétés [sys_properties] lorsque les paramètres de sécurité élevée sont actifs :

- **read_roles** : une liste de noms de rôles séparés par des virgules qui sont autorisés à lire tous les champs de cette propriété.
- **write_roles** : une liste de noms de rôles, séparés par des virgules, qui sont autorisés à écrire/modifier tous les champs de cette propriété.

Les propriétés répertoriées dans la table Propriétés ont **des read_roles** d'administrateur et des **write_roles** de security_admin. Les utilisateurs disposant du rôle administrateur peuvent afficher et lire les valeurs de propriété, mais ils doivent accéder au rôle security_admin pour les modifier.

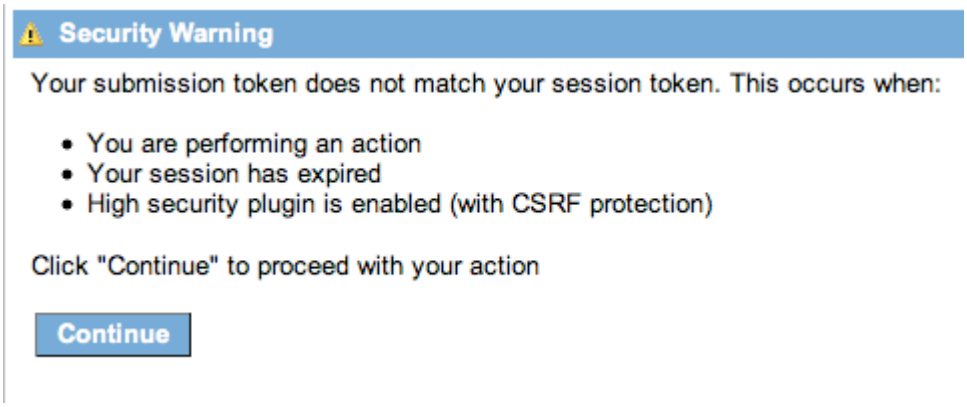
Notifications

L'activation des paramètres de sécurité élevée active également les messages d'avertissement de sécurité. Voici un exemple de message qui s'affiche après une approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notification d'avertissement de sécurité



Propriétés des paramètres de sécurité élevée

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.ui.escape_text	Valeurs XML d'échappement au niveau de l'analyseur de l'interface utilisateur. Prévient les attaques de script de site à site réfléchies et stockées. Cette propriété n'est pas applicable dans Portail de services. **Remarque :** Cette propriété est définie sur **vrai** par défaut dans les Vancouver versions ultérieures et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez l'assistance clientèle.	Oui	Balisage XML d'échappement [Mis à jour dans Centre de sécurité 1.3]
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans les balises Jelly JavaScript	Oui, dans les nouvelles instances	Script Jelly d'échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	<![CDATA[<script type="text/javascript">]]> . Applique l'échappement uniquement si l'attribut type dans la <![CDATA[<script>balise]]> est vide ou si la valeur est text/javascript, text/ecmascript, application/javascript, application/ecmascript ou application/x-javascript.		
glide.ui.rotate_sessions	Effectuez une rotation des identificateurs de session HTTP pour réduire les vulnérabilités de sécurité. Voir : http://www.owasp.org/index.php/Session_Management#Rota .	Oui **Remarque :** Si vous utilisez le module d'extension SAML 2.0 pour l'authentification unique, définissez cette propriété sur Non. Sinon, cela interfère avec le partage d'informations de session qui a lieu entre l'instance et le fournisseur d'identité.	Rotation des identificateurs de session HTTP
glide.ui.secure_cookies	Activer les cookies de session sécurisés : Activer une sécurité supplémentaire par les cookies. Si **oui**, la validation stricte des cookies de session s'applique.	Oui	Appliquer la sécurité stricte des cookies de session [Mis à jour dans Centre de sécurité 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.security.password_reset.uri	Pour mobile Réinitialisation du mot de passe, URL vers laquelle l'utilisateur est redirigé lorsqu'il clique sur le bouton **Mot de passe oublié ?** .		Aucun
glide.security.strict.updates	Vérifiez à deux reprises la sécurité des transactions entrantes lors de la soumission d'un formulaire (les droits sont toujours vérifiés lors de la création d'un formulaire). **Remarque :** Cette propriété est définie sur **vrai** par défaut dans les Vancouver versions ultérieures et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez l'assistance clientèle.	Oui	Double vérification des transactions entrantes [Mis à jour dans Centre de sécurité 1.3]
glide.security.strict.actions	Vérifiez les conditions des actions d'interface utilisateur avant leur exécution. Normalement, les conditions sont vérifiées uniquement lors du rendu du formulaire.	Oui	Vérifier les conditions de l'action de l'interface utilisateur avant son exécution
glide.security.use_csrf_token	Activez l'utilisation d'un jeton de sécurité pour	Oui	Activer le jeton anti-CSRF [nouveau dans Security Center 1.3, mis à jour dans la version 1.5 et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.		supprimé dans la version 2.0]
glide.ui.escape_html_list_field	HTML d'échappement pour les champs HTML d'une vue de liste.	Oui	HTML d'échappement dans les vues de listes [Mis à jour dans Centre de sécurité 1.3 et 1.5]
glide.html.escape_script	Balises JavaScript d'échappement dans les champs HTML.	Oui	Échapper à JavaScript [mis à jour dans Centre de sécurité 1.3]
glide.ui.forgetme	Décochez la case **Se souvenir de moi** de la page de connexion.	Oui	Supprimer Se souvenir de moi
glide.smtp.auth	Authentifiez-vous auprès du serveur SMTP à l'aide des propriétés du nom d'utilisateur et du mot de passe. **Remarque :** Cette propriété est obsolète.	Oui	Authentification SMTP (obsolète)
glide.soap.strict_security	Appliquez une sécurité stricte sur les demandes SOAP entrantes. Exige que les demandes SOAP entrantes passent par le gestionnaire de sécurité pour l'accès à la table et au champ et vérifie que les utilisateurs SOAP possèdent les rôles appropriés pour utiliser le service Web.	Oui	Appliquer la sécurité stricte des requêtes SOAP [Mis à jour dans Centre de sécurité 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.basicauth.required.wsdl	Demandez une autorisation pour les demandes WSDL entrantes. **Remarque :** Si vous choisissez de ne pas exiger d'autorisation pour les demandes WSDL entrantes, vous devez modifier les règles de contrôle d'accès (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.	Oui	Exiger une autorisation pour la demande WSDL [Mis à jour dans Centre de sécurité 1.3 et 1.5]
glide.basicauth.required.csv	Exiger une autorisation de base pour les demandes CSV entrantes .	Oui	Exiger une autorisation pour les demandes CSV [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.excel	Demandez une autorisation de base pour les demandes Excel entrantes.	Oui	Exiger une autorisation pour les demandes Excel [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.importprocessor	Demandez l'autorisation de base pour les demandes d'importation entrantes.	Oui	Exiger une autorisation pour les demandes d'importation [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.pdf	Demandez une autorisation de base pour les demandes PDF entrantes.	Oui	Exiger une autorisation pour les demandes PDF [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.rss	Demandez l'autorisation de base pour les demandes RSS entrantes.	Oui	Exiger une autorisation pour les demandes RSS [Mis à jour dans Centre de sécurité 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.basicauth.required.scriptedprocessor	Demandez une autorisation de base pour les demandes de script entrantes.	Oui	Exiger une autorisation pour les demandes de script [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.soap	Demandez l'autorisation de base pour les demandes SOAP entrantes.	Oui	Exiger une autorisation pour les demandes SOAP [Mis à jour dans Centre de sécurité 1.3, 1.5 et 2.0]
glide.basicauth.required.unl	Demandez une autorisation de base pour les demandes de déchargement entrantes.	Oui	Exiger une autorisation pour les demandes de déchargement [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.xml	Demandez l'autorisation de base pour les demandes XML entrantes.	Oui	Exiger une autorisation pour les demandes XML [Mis à jour dans Centre de sécurité 1.3]
glide.basicauth.required.xsd	Demandez l'autorisation de base pour les demandes XSD entrantes.	Oui	Exiger une autorisation pour les demandes XSD [Mis à jour dans Centre de sécurité 1.3]
glide.cms.catalog_uri_relative	Appliquez des liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si **oui**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du `uri` paramètre. Si **non**, toutes les URL sont autorisées, ce qui permet la liaison à un contenu externe non autorisé.	Oui	Renforcer les liens relatifs [Mis à jour dans Centre de sécurité 1.3 et 1.5]
glide.set_x_frame_options	Activez cette propriété pour définir l'en-tête de réponse X-Frame-Options sur SAMEORIGIN	Oui	Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mis à jour dans Centre de sécurité 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	pour toutes les pages de l'interface utilisateur. L'en-tête de réponse HTTP X-Frame-Options peut être utilisé pour indiquer si un navigateur doit être autorisé à afficher une page dans un ou <iframe>un <frame> . Les sites peuvent utiliser cette propriété pour éviter les attaques de détournement de clic, en s'assurant que leur contenu n'est pas incorporé dans d'autres sites. https://developer.mozilla.org/en/the_x-frame-options_response_header		
glide.ui.attachment.download_mime_types	Une liste de types MIME de pièce jointe séparés par des virgules qui ne sont pas alignés dans le navigateur. Prévient les attaques de script de site à site. Par exemple, text/html force le téléchargement des fichiers HTML sur le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur.	text/html,image/svg,image/svg+xml	Restreindre les types MIME téléchargeables [Mis à jour dans Centre de sécurité 1.3 et 2.0]
glide.security.groupby_acl_check	Lorsque cette propriété est activée, les vérifications d'ACL pour les opérations Grouper par sont effectuées pour les noms de	Oui	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	groupe en fonction des données réelles des groupes.		
glide.security.diag_txns_acl	Si **oui**, seul l'utilisateur administrateur ou l'utilisateur de l'adresse IP autorisée peut accéder à stats.do, threads.do et replication.do.	Non	Restreindre l'accès à la surveillance des performances [Mis à jour dans Centre de sécurité 1.3]
glide.ui.security.codetag.allow_script	Autorisez le HTML incorporé (utilisant des balises [code]) pour contenir les balises JavaScript. **Remarque :** Cette propriété est définie sur **vrai** par défaut dans les Vancouver versions ultérieures et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez l'assistance clientèle.	Non	Désactiver le code HTML intégré [Mis à jour dans Centre de sécurité 1.3]
glide.script.allow.ajaxevaluate	Activez le processeur AJAXEvaluate. L'appel d'API *AJAXEvaluate* permet au client d'envoyer et d'exécuter des scripts arbitraires sur le serveur.	Non	Désactiver AJAXEvaluate

Les propriétés suivantes sont définies dans la table sys_properties, mais ne sont pas visibles sur la page Paramètres de sécurité élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
com.glide.communications.httpclient.verify_hostname	Vérifiez le nom d'hôte et la chaîne de certification présentés par les hôtes SSL distants. Protégez-vous contre les attaques de l'homme du milieu (MITM). Pour plus d'informations, consultez la section Configuration du spoke Kubernetes **Remarque :** Cette propriété remplace la propriété com.glide.communications.trustmanager_trust_all.	vrai	Aucun
glide.basicauth.required.schema	Demandez l'authentification de base pour les demandes de schéma de table entrantes.	vrai	Aucun
glide.security.csrf_previous.autoriser	Autorisez l'utilisation d'un jeton de sécurité expiré pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.	Faux	Aucun
glide.security.csrf_previous.time_limit	Délai en secondes avant l'expiration d'un jeton de sécurité. Permet de contrôler la durée de validité du jeton CSRF précédent. Lorsque	86400 **Remarque :** Valeur en secondes. Équivalent à 1 jour.	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	la session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la *glide.security.csrf_previous.allow* propriété est activée et dans la période décrite dans cette propriété. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.		
glide.security.csrf.strict.validation.mode	Applique une validation stricte sur les jetons CSRF afin que les utilisateurs ne puissent pas soumettre à nouveau une demande si le jeton CSRF ne correspond pas.	Faux	Empêcher les utilisateurs d'accepter l'avertissement pour contourner la validation CSRF [Mis à jour dans Centre de sécurité 1.3 et 1.5]
com.glide.security.check_unapplied_html	Applique le comportement de nettoyage des champs de translated_html à un niveau global pour les affectations de champs.	appliquer	Aucun

Activation des paramètres de sécurité élevée

Le module d'extension Paramètres de sécurité élevée est actif par défaut sur toutes les nouvelles instances. S'il n'est pas actif sur votre instance, vous pouvez demander le module d'extension.

Avant de commencer
Rôle requis : aucun

Avant d'activer les paramètres de sécurité élevée sur une instance existante :

1. Passez en revue les informations suivantes pour comprendre le nouveau comportement :
   - Règles de la liste de contrôles d'accès
   - Paramètres de sécurité élevée
   - Propriété de refus par défaut
2. Activez le module d'extension sur une instance de non-production. Un clone récent de la production est préférable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

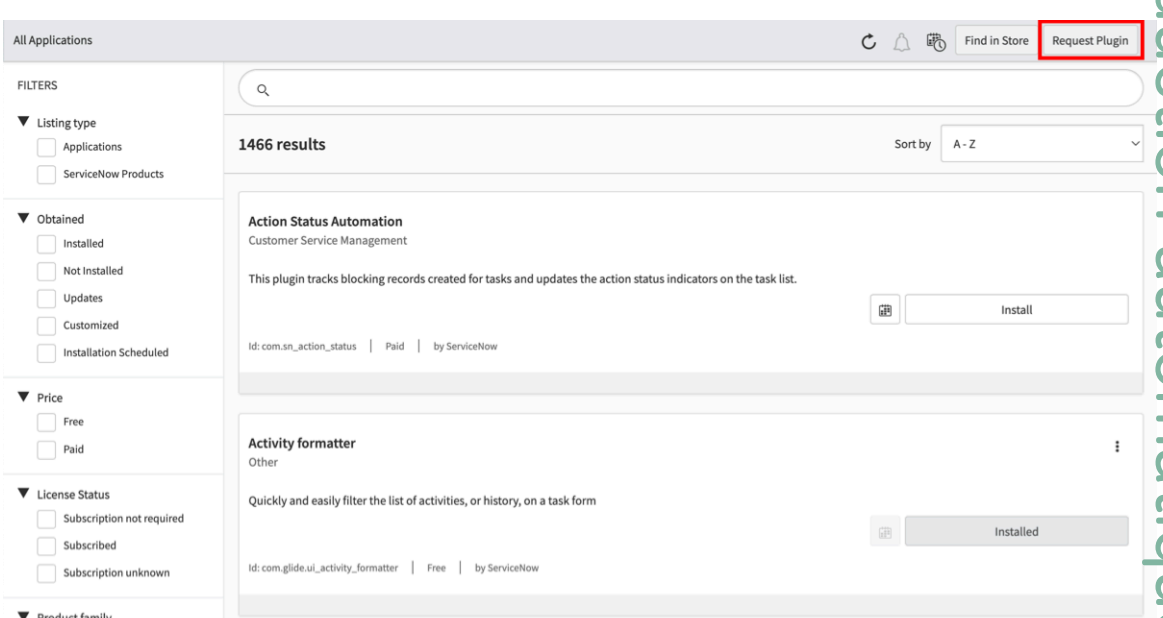
3. Testez la fonctionnalité révisée, en particulier les ACL ajoutées et la fonctionnalité de refus par défaut. Continuez les tests jusqu'à ce que le système fonctionne comme prévu. Si les utilisateurs ne peuvent pas accéder aux ressources attendues, assurez-vous qu'ils disposent des rôles et des règles ACL appropriés pour leur accorder l'accès.
4. Créez des ensembles de mises à jour de tous les changements nécessaires afin de pouvoir les appliquer à la production.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Activer le module d'extension de haute sécurité [mis à jour dans Centre de sécurité 1.3] Paramètres de la sécurisation renforcée de la sécurité de l'instance.

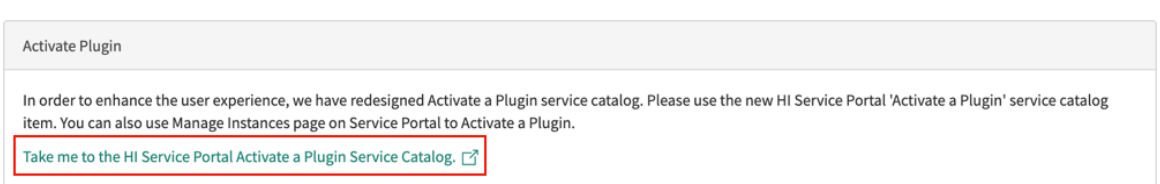
Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

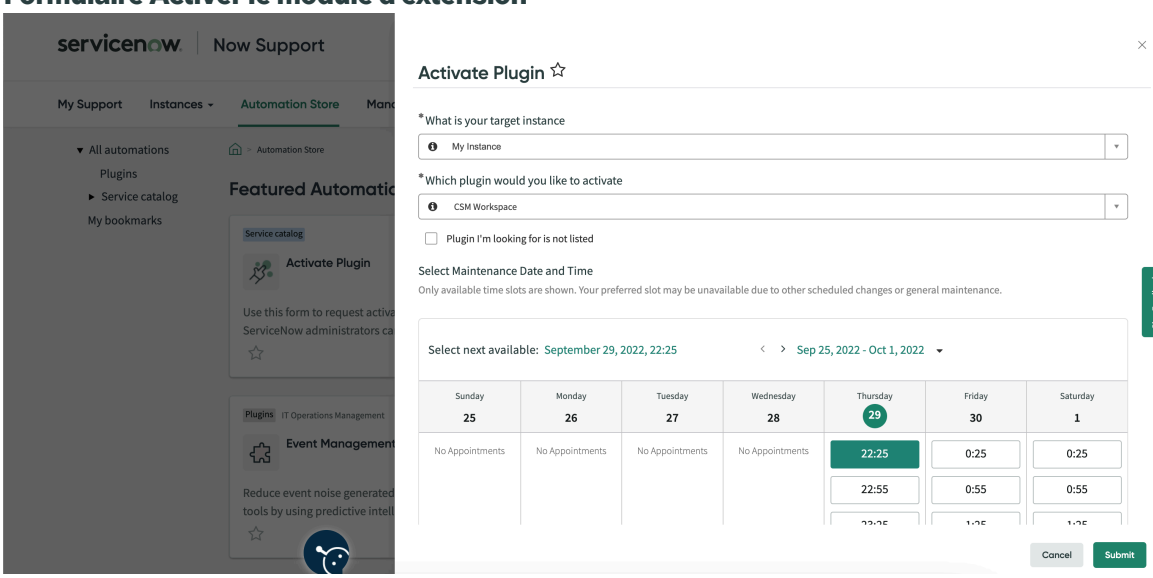
Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Soumettre**.
   Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

VPN (Virtual Private Network)

Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.

Explorer



Découvrez les fonctionnalités et les valeurs commerciales du réseau privé virtuel.

Activer



Active le réseau privé virtuel.

Configurer



Découvrez comment configurer un réseau privé virtuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer le réseau privé virtuel (VPN)

Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.

Mes informations IP

Lors de la configuration d'une intégration qui utilise un protocole chiffré, tel que LDAP (Lightweight Directory Access Protocol) ou HTTPS, il est recommandé d'utiliser Internet comme mécanisme de transport.

Cependant, il peut y avoir des exigences de sécurité ou d'architecture réseau qui dictent l'utilisation d'une connexion de réseau privé virtuel (VPN) de sécurité de protocole Internet (IPSEC) de site à site entre les centres de données et vos réseaux d'entreprise. Le VPN prend en charge la communication chiffrée nécessaire entre l'instance et votre réseau.

⚠ Avertissement :

Lorsqu'un tunnel VPN est initié, il fonctionne comme une connexion de site à site. Cela signifie que le point de terminaison de votre infrastructure reçoit une adresse IP, appelée domaine de chiffrement. Cette adresse IP publique est accessible par n'importe quelle instance au sein d'un même centre de données.

Par exemple, si vous disposez d'un service Web interne et que vous établissez un tunnel VPN, votre instance est en mesure d'atteindre le point de terminaison interne ainsi que toutes vos autres instances dans le même centre de données.

Connexions VPN

L'infrastructure ServiceNow VPN utilise des paires d'appareils Cisco Adaptive Security Appliance (ASA) qui servent de points de terminaison VPN.

Le VPN entre l'instance et votre réseau utilise votre matériel réseau existant pour prendre en charge les communications. Il n'est pas nécessaire d'installer un matériel. Étant donné que chaque client dispose d'une configuration unique, l'instance dispose d'une solution VPN flexible. l'instance a créé des tunnels vers Checkpoint, Juniper, Nortel et d'autres appareils compatibles VPN IPSEC.

Les connexions VPN entre l'instance et votre réseau sont créées pour prendre en charge le flux chiffré du trafic dans votre réseau. Souvent, les intégrations qui utilisent le VPN n'ont pas de cryptage dans le cadre du protocole sous-jacent. Par exemple, LDAP sur le VPN par rapport à LDAPS sur Internet et HTTP sur le VPN par rapport à HTTPS sur Internet.

Le réseau n'autorise aucun trafic entrant vers l'intégration ServiceNow ou d'utilisateur final vers ServiceNow à traverser une connexion VPN. Cette communication restreinte comprend l'accès de l'utilisateur final à la plateforme, l'administration de la plateforme, les intégrations de services Web et d'autres intégrations configurées pour utiliser un serveur MID. Toutes ces communications entrantes vers l'instance doivent être effectuées via Internet à l'aide du protocole HTTPS. Cette configuration fournit un canal de communication chiffré. Le canal de chiffrement, ainsi que le contrôle d'accès IP, répondent aux exigences de sécurité pour ce flux de trafic.

Adresses pour la communication VPN

Pour éviter les conflits ou les chevauchements avec les réseaux internes ServiceNow ou avec d'autres schémas d'adresses IP internes de votre réseau, tout le trafic tunnelisé dans le domaine de chiffrement doit utiliser des adresses non RFC-1918 des deux côtés du tunnel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow fournit une adresse IP unique pour la source des requêtes sur votre réseau. Vous devez fournir des traductions d'adresses réseau (NAT) non RFC-1918 pour chaque hôte qui s'intègre à votre instance. Ces adresses publiques doivent appartenir à votre organisation. Les adresses tierces ne peuvent pas être utilisées à l'intérieur des tunnels. De plus, le domaine de chiffrement ne doit pas contenir l'adresse IP de l'homologue VPN.

Tunnels redondants

Il existe deux façons de créer une redondance pour vos tunnels :

- Vous utilisez le même domaine de chiffrement derrière vos deux pairs. Il s'agit de la méthode privilégiée.
- Utilisation d'un domaine de chiffrement différent derrière chaque homologue.

Avec la première méthode, vous devez fournir la même adresse NAT derrière chacun de vos pairs pour créer un chemin de connexion à l'aide de cette adresse à votre serveur. Le chemin vers votre serveur peut être la même machine physique ou un miroir qui fournit des services identiques. Avec cette méthode, votre instance utilisera la même adresse IP pour se connecter à vos serveurs, que votre tunnel primaire ou secondaire soit actif. Si vous avez plusieurs serveurs, suivez le même schéma pour vos serveurs supplémentaires. Cette méthode offre le plus de transparence à vos utilisateurs et est recommandée.

La deuxième méthode nécessite une configuration dans votre instance pour assurer la redondance. Lorsque le tunnel est utilisé pour LDAP, par exemple, vous pouvez fournir des serveurs LDAP redondants dans votre instance. Notez que cette méthode exige que la connexion au premier serveur LDAP configuré expire avant que l'instance ne tente de se connecter au serveur secondaire. En raison de ce délai supplémentaire, cette solution ne doit être mise en œuvre que si la première option est inaccessible. Notez également que tous les services ne peuvent pas être configurés de manière redondante dans votre instance. Si vous utilisez un tunnel VPN pour autre chose que LDAP et qu'une redondance est requise, vérifiez que votre configuration peut prendre en charge plusieurs adresses, ou consultez la première option ci-dessus.

Alternatives à l'utilisation d'un VPN

Ces alternatives simplifient la connexion de votre instance aux ressources des ServiceNow centres de données et offrent un meilleur chiffrement. En outre, vous pouvez éviter les problèmes que les temps d'arrêt du VPN pourraient causer, tels que rendre votre instance indisponible pour les utilisateurs en cas de problème avec le tunnel VPN.

Authentification unique (SSO) et MID Server

Envisagez d'utiliser une combinaison de Single Sign-On (SSO) pour l'authentification et du serveur MID pour la synchronisation des données utilisateur, plutôt que d'utiliser un VPN pour connecter votre serveur LDAP à votre instance. Pour les intégrations autres que LDAP, envisagez d'utiliser le chiffrement basé sur un certificat.

Vous pouvez utiliser l'écouteur LDAP sur un serveur MID pour synchroniser votre table d'utilisateurs en temps quasi réel.

L'avantage de cette approche est qu'il n'y a pas de trous de pare-feu, de routes, de tunnels VPN ou d'autres paramètres réseau spéciaux à configurer et à maintenir. La solution SSO/MID-Server est la méthode la plus flexible, la plus sécurisée et la plus rentable pour réaliser l'intégration LDAP complète.

LDAP sur SSL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une autre alternative à l'utilisation d'un tunnel VPN consiste à configurer LDAP Over SSL (LDAPS) directement sur Internet. Vous pouvez configurer un contrôleur de domaine en lecture seule et verrouiller l'instance dans votre DMZ en utilisant uniquement les adresses source de l'instance et les ports de destination de votre choix. Étant donné que les ports LDAP sont configurables dans votre instance, vous pouvez effectuer une traduction d'adresse de port (PAT) si vous le souhaitez. Avec LDAPS, vous contrôlez le certificat qui est téléchargé via un canal chiffré vers l'instance, (voir Chargement d'un certificat sur une instance). Les paquets ne peuvent pas être chiffrés ou déchiffrés sans le certificat.

L'avantage de cette approche est qu'elle fournit un mécanisme de cryptage et de décryptage plus puissant. Un VPN ne peut crypter et déchiffrer le trafic entre les deux pairs assis sur Internet qu'avec une clé pré-partagée coordonnée, similaire à un mot de passe. LDAPS fournit un chemin chiffré plus long, de bout en bout, au niveau de la couche applicative et avec un certificat beaucoup plus compliqué qu'une clé prépartagée utilisée par le tunnel IPSec.

Configuration VPN

À partir du moment où une demande VPN est soumise, il faut généralement une semaine ou moins pour terminer la construction du VPN. Pour prendre en charge les exigences de redondance de votre instance et de votre organisation, un minimum de deux et un maximum de quatre VPN sont provisionnés (du site actif au vôtre ou du site actif à votre site de récupération d'urgence, et ainsi de suite).

Il est recommandé que le domaine de chiffrement soit aussi précis que possible. Idéalement, le domaine de chiffrement n'inclurait que les hôtes spécifiques requis pour les intégrations. Un grand domaine de cryptage peut créer des opportunités de divergences de routage (VPN contre Internet).

Pour créer le VPN, l'instance effectue les opérations suivantes :

1. Fournit les adresses de l'homologue VPN et de l'hôte de chaque centre de données.
2. Construit la connectivité VPN nécessaire à partir de deux centres de données dans votre réseau. Pour répondre aux exigences de redondance et de reprise après sinistre (DR), les VPN peuvent être provisionnés à partir de deux centres de données sur deux réseaux.

L'instance ne prend pas en charge la construction de plusieurs tunnels VPN dans un réseau client dans le but de se connecter à plusieurs régions géographiques ou filiales. Vous devez effectuer tout routage intersite, distribution ou mise en forme du trafic au sein de votre propre réseau interne, plutôt que d'avoir plusieurs tunnels VPN.

Activer un service VPN

Pour toutes les demandes de VPN, y compris la mise en service, les modifications ou les questions d'ordre général, utilisez le formulaire de demande de VPN de Catalogue de services.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à https://support.servicenow.com/now?draw=case.
2. Sélectionnez l'onglet **Automation Store** .
3. Utilisez l'arborescence de gauche pour accéder à **Toutes les automatisations** > **Catalogue de services** > **Infrastructure de cloud**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Sélectionner les demandes VPN**
5. Sélectionnez le type de demande VPN approprié.
6. Répondez aux questions.
   Les questions varient en fonction du type de demande sélectionné.
7. Cliquez sur **Envoyer**.

Résultats

Une fois votre demande soumise, ServiceNow nous travaillerons avec votre ou vos ingénieurs réseau pour tester et valider que le VPN transmet correctement le trafic. Pour vous assurer que vous recevrez une réponse à vos questions en temps opportun, veuillez répondre aux questions relatives au VPN au cours de ce processus.

Configuration d'une adresse pour la communication VPN

Pour éviter les conflits ou les chevauchements avec les réseaux internes ServiceNow ou avec les schémas d'adresses IP internes d'un autre client, l'instance exige que tout le trafic tunnelisé dans le domaine de chiffrement utilise des adresses non-RFC-1918 des deux côtés du tunnel.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'instance fournit une adresse IP unique pour la source des requêtes sur votre réseau.

Procédure

Fournissez des adresses de traduction d'adresses réseau (NAT) non RFC-1918 pour chaque hôte qui s'intègre à l'instance.

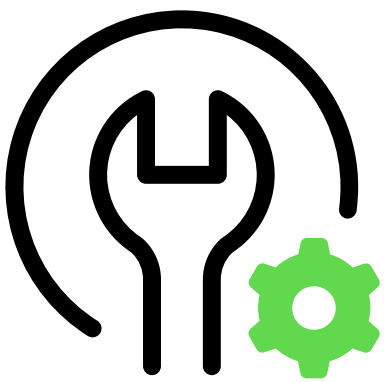
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

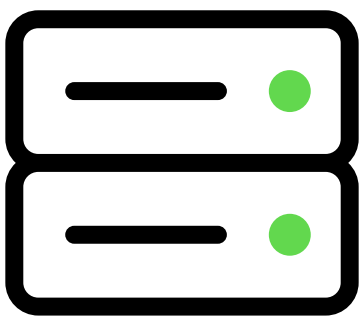
Autres paramètres et ressources de sécurité

Cette section contient des propriétés de sécurité que vous avez définies en dehors du Centre de sécurité de l'instance, ainsi que d'autres ressources liées à la sécurité.



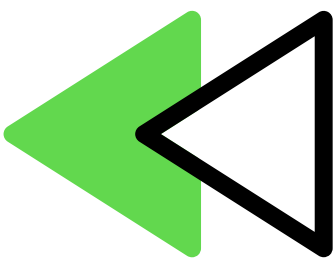
Propriétés système de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.



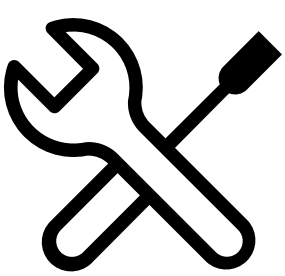
Guide de déploiement du Serveur MID

Le serveur ServiceNow Management, Integration, and Discovery (MID) est une application Java légère qui s'exécute en tant que service Windows ou démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.



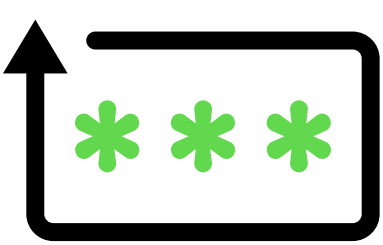
Comportement réversible

Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».



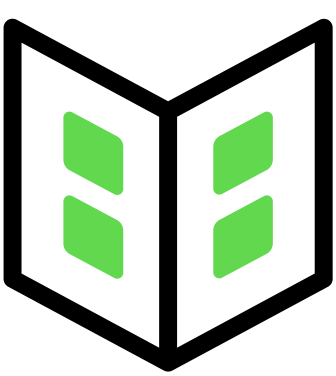
Propriétés de sécurité dépréciées

Ces propriétés de sécurité ont été déconseillées dans les versions précédentes.



Utilisation du contrôle d'accès au contenu JavaScript

Vous pouvez utiliser le contrôle d'accès au contenu JavaScript pour modifier la liste des URL JavaScript tierces bloquées au sein de votre instance.



Autres ressources de sécurisation renforcée de la sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

		Autres sources d'information sur le renforcement des contrôles de sécurité, en ce qui concerne le ServiceNow AI Platform .

Propriétés des paramètres de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.

Il existe plusieurs façons de définir ou de modifier les propriétés des paramètres de sécurité généraux.

- Accédez à la **Propriétés système** > **Sécurité**.

  Les options de la page Sécurité sont **Oui** ou **Non**.

- Accédez à **sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **définies sur vrai** ou **faux**.

- Accédez à la **Sécurité de système** > **Centre de sécurité de l'instance**, puis cliquez sur **Sécurisation renforcée**.

  Vous pouvez configurer les paramètres des propriétés de sécurité les plus importantes et les plus critiques. Le contenu des paramètres de renforcement de la sécurité de l'instance contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le ServiceNow AI Platform. Pour en savoir plus sur chacune de ces propriétés, reportez-vous à la section Paramètres de sécurisation renforcée.

⚠ Avertissement :
Lors de l'implémentation de l'une de ces fonctionnalités de sécurité, vous devez tester minutieusement les fonctionnalités avant de les déployer dans une instance de production.

Prise en charge de l'échappement et du script incorporé

glide.ui.security.allow_codetag	Prend en charge l'incorporation du code HTML à l'aide de la balise [code]. Valeur par défaut : oui **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Désactiver le code HTML intégré [Mis à jour dans Centre de sécurité 1.3]
glide.ui.security.codetag.allow_script	Permet au HTML incorporé (utilisant des balises [code]) de contenir des balises JavaScript.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Remarque : Cette propriété est définie sur **vrai** par défaut dans les Vancouver versions ultérieures et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez l'assistance clientèle. Pour en savoir plus, voir Désactiver les balises JavaScript dans le HTML intégré [Mis à jour dans Centre de sécurité 1.3].
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans les balises Jelly JavaScript <![CDATA[<script type="text/javascript">]]> . Applique l'échappement uniquement si l'attribut type dans la <![CDATA[<script>balise]]> est vide ou si la valeur est text/javascript, text/ecmascript, application/javascript, application/ecmascript ou application/x-javascript. • Valeur par défaut : ◦ Instances nouvelles/zbootées : true ◦ Instances mises à niveau : false • Valeur recommandée : oui **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Script Jelly d'échappement [Mis à jour dans Centre de sécurité 1.3 et 1.5]

Limites et comportement des pièces jointes

com.glide.attachment.max_size	Définit la taille maximale de la pièce jointe en mégaoctets.
glide.attachment.role	Répertorie les rôles (séparés par des virgules) qui peuvent créer des pièces jointes.
glide.attachment.extensions	Répertorie les extensions de fichier (séparées par des virgules) qui peuvent être jointes aux documents via la boîte de dialogue de pièce jointe. Les extensions ne doivent pas inclure le point (.). Par exemple, xls, xlsx, doc, docx. Laissez vide pour autoriser toutes les extensions. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Fichiers et ressources
glide.ui.attachment.force_download_all_mime_types	Force le téléchargement de tous les fichiers de pièce jointe de type MIME (Multipurpose Internet Mail Extensions).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Valeur par défaut : • Instances nouvelles/zbooted : Oui • Instances mises à niveau : non **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Définir les types MIME enfant autorisés [nouveau dans Centre de sécurité 2.0]
glide.security.file.mime_type.validation	Active (**Oui**) ou désactive (**Non**) la validation du type MIME pour les pièces jointes. Le type MIME est vérifié pour les extensions de fichier configurées via `glide.attachment.extensions` pendant le chargement. Valeur par défaut : • Instances nouvelles/zbooted : Oui • Instances mises à niveau : non **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Restreindre les types MIME chargés [Mis à jour dans Centre de sécurité 1.3 et 2.0]

Chargements du client

Ces propriétés affectent uniquement les téléchargements des clients. Ils n'affectent pas les pièces jointes.

glide.ui.strict_customer_uploaded_static_content	Lorsque vous définissez cette propriété sur **Oui**, active la possibilité de restreindre les types de fichiers qui peuvent être téléchargés, lorsqu'ils ont été téléchargés à l'aide de la fonctionnalité Charger un fichier de l' ServiceNow AI Platform. Utilisé avec `glide.ui.strict_customer_uploaded_content_types` **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Restreindre les types de fichiers téléchargeables dans le contenu statique [Mis à jour dans Centre de sécurité 1.3]
glide.ui.strict_customer_uploaded_content_types	Lorsque ce paramètre inclut une liste de types de fichiers délimités par des virgules, seuls ces types de fichiers peuvent être

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	téléchargés à ServiceNow AI Platform partir de l'instance. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Restreindre les types de fichiers téléchargeables dans le contenu statique [Mis à jour dans Centre de sécurité 1.3]

Gestionnaire de sécurité et options

glide.security.manager	Gestionnaire de sécurité.
glide.sm.default_mode	Comportement par défaut du gestionnaire de sécurité en l'absence de tout ACL dans une table.
glide.security.strict.updates	Revérifie la sécurité des transactions entrantes durant la soumission du formulaire. Les droits sont toujours vérifiés lors de la création d'un formulaire. **Remarque :** Cette propriété est définie sur **vrai** par défaut et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez l'assistance clientèle. Pour en savoir plus, voir Double vérification des transactions entrantes [Mis à jour dans Centre de sécurité 1.3].
glide.security.strict.actions	Vérifie les conditions des actions d'interface utilisateur avant leur exécution. Normalement, les conditions ne sont vérifiées que pendant le rendu du formulaire. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Vérifier les conditions de l'action de l'interface utilisateur avant son exécution
glide.security.granular.create	Applique les règles de création sur les nouveaux enregistrements (par opposition aux règles d'écriture, qui peuvent inclure la création et la mise à jour).
glide.security.explain.write.locks	Affiche une explication dans les éléments de formulaire verrouillés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cookies

glide.ui.forgetme	Supprime la case à cocher **Se souvenir de moi** de la page de connexion lorsque l'instance utilise des connexions LDAP ou DB. Les sessions connectées actives de l'utilisateur expirent après X minutes d'inactivité, où X est la valeur de la propriété système **glide.ui.session_timeout** . Valeur par défaut : Oui (instances nouvelles et démarrées Z) **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Supprimer Se souvenir de moi
glide.ui.secure_cookies	Active les cookies de session sécurisés pour appliquer une sécurité supplémentaire par les cookies. Si **oui**, la validation stricte des cookies de session s'applique. Avec les cookies de version 3 activés, des exigences de sécurité supplémentaires sont également appliquées. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Appliquer la sécurité stricte des cookies de session [Mis à jour dans Centre de sécurité 1.3]
glide.secure_cookie.debug	Débogage de cookies de session sécurisée. Sélectionnez cette option pour permettre la journalisation de débogage extensive des opérations de cookies de session sécurisée.

Restrictions de sécurité pour l'exécution de scripts en provenance du client

glide.script.allow.ajaxevaluate	Active le processeur AJAXEvaluate. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Désactiver AJAXEvaluate
glide.script.secure.ajaxgliderecord	Applique des listes de contrôle d'accès (ACL) de sécurité standard aux appels AJAXGlideRecord.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Valeur par défaut : oui, pour les instances nouvelles et mises à niveau. (Si **Oui**, ne peut pas être remplacé par **Non**.) **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Exiger la vérification de l'ACL AJAXGlideRecord [Mis à jour dans Centre de sécurité 1.3]

Divers

com.glide.communications.trustmanager_trust_all	Par défaut, l'instance fait confiance à l'autorité de certification (CA) d'un certificat. Garantit que l'instance accepte les certificats auto-émis. Pour valider l'autorité de certification d'un certificat, définissez cette propriété sur **Non** Paramètres de la sécurisation pour la sécurité de l'instance : Renforcer l'approbation de certificat [Mis à jour dans Centre de sécurité 1.3, supprimé dans la version 2.0, ajouté dans la version 7.0]
glide.outbound.sslv3.disabled	Lorsqu'elle est active, force les connexions sortantes d'une instance à utiliser le protocole TLS (Transport Layer Security) au lieu du SSL (secure sockets layer). Paramètres de la sécurisation pour la sécurité de l'instance : Désactiver les connexions SSLv2/SSLv3 sortantes [Mis à jour dans Centre de sécurité 1.3] **Important :** La valeur de cette propriété est un remplacement sûr et ne peut pas être modifiée une fois modifiée.

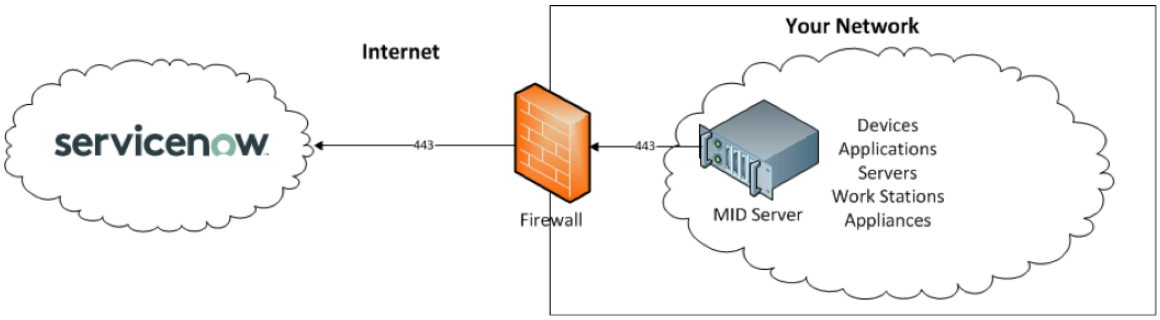
Des propriétés supplémentaires sont disponibles pour Paramètres de sécurité élevée.

Guide de déploiement sécurisé de MID Server (renforcement de la sécurité de l'instance)

Le ServiceNow Serveur MID (Management, Integration, and Discovery) est une application Java légère qui exécute un service Windows ou un démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Il s'authentifie en toute sécurité auprès de votre instance dans le Cloud à l'aide ServiceNow de ses propres identifiants de connexion, et facilite la transmission des données avec vos applications, sources de données et services. Plusieurs serveurs MID peuvent être déployés dans différents segments du réseau pour fournir une évolutivité supplémentaire.

Prenez en compte les facteurs suivants concernant la sécurité de votre serveur MID :

Sécurité physique

Sécurisez le matériel physique qui héberge le serveur MID ou l'hyperviseur pour les serveurs MID virtualisés.

- Placez le matériel dans un emplacement sécurisé qui protège le matériel contre tout accès non autorisé.
- Protégez l'accès à cet emplacement avec un lecteur de carte électronique et une surveillance par vidéosurveillance.
- Placez le matériel physique dans une cage verrouillée ou un rack avec contrôle d'accès par clé physique.

Sécurité de l'infrastructure virtuelle

Utilisez la virtualisationavec la flexibilité d'installer plusieurs serveurs MID dans des systèmes d'exploitation virtualisés et des réseaux dans du matériel physique partagé.

L'accès à l'hyperviseur et aux consoles de gestion de l'infrastructure virtuelle doit être protégé pour empêcher le clonage non autorisé du serveur MID virtualisé :

- Limitez l'accès à l'hyperviseur et aux consoles de gestion de l'infrastructure virtuelle par quelques administrateurs de confiance.
- Autorisez uniquement les connexions au réseau approuvé interne pour la console de gestion, telle que ESX Server et VirtualCenter.
- Utilisez les VLAN pour prévenir les attaques réseau.
- Suivez les directives de sécurité publiées dans les guides de sécurisation renforcée de la virtualisation des fournisseurs.

Sécurité du système d'exploitation

Découvrez comment le MID Server stocke son nom d'utilisateur et son ServiceNow AI Platform mot de passe dans son fichier de configuration, nommé config.xml, pour une authentification sécurisée à l'instance.

Le Serveur MID doit être déployé dans un système d'exploitation sécurisé et renforcé pour assurer la protection contre tout accès non autorisé aux informations d'identification :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Limitez l'accès au système d'exploitation à quelques administrateurs de confiance.
- Surveillez les journaux du système d'exploitation pour détecter tout accès non autorisé, en particulier les tentatives d'accès au fichier config.xml, car ce fichier contient des informations importantes sur la configuration du serveur MID.
- Installez régulièrement les correctifs de sécurité du système d'exploitation avec les logiciels antivirus les plus récents et mettez régulièrement à jour les définitions des antivirus.
- Le serveur MID nécessite une infrastructure Java actuelle pour s'exécuter. Gardez Java à jour régulièrement.
- Supprimez ou désactivez les services et applications inutiles.
- Installez un pare-feu de système d'exploitation pour limiter l'accès aux ports non autorisés.
- Suivez les directives de sécurité publiées dans les guides de sécurisation renforcée du système d'exploitation des fournisseurs.

Sécurité réseau

Le serveur MID communique sur le port 443 à l'aide de SSL avec l'instance et ne requiert aucune connexion entrante.

Pour sécuriser correctement votre serveur MID dans un réseau, procédez comme suit :

- Installez le Serveur MID sur un serveur sécurisé derrière un pare-feu d'entreprise pour vous protéger contre tout accès non autorisé à partir d'Internet.
- Configurez le pare-feu sur Serveur MID pour qu'aucune connexion entrante n'accepte d'autres connexions que celles requises pour la gestion du système d'exploitation et du matériel en entreprise.
- Le système qui héberge le serveur MID doit pouvoir accéder au site de téléchargement à **install.servicenow.com**ServiceNow.

> **Remarque :**
> Cette URL renvoie au site de téléchargement, qui n'est ServiceNow pas accessible à partir de cette rubrique.

L'ordinateur hôte MID Serve doit pouvoir accéder à ce site pour télécharger le package d'installation. Il **install.servicenow.com** contacte toutes les 60 minutes pour voir si une version plus récente est disponible et si c'est le cas, il effectue une mise à niveau automatique. Une mise à niveau de Serveur MID a également lieu lorsque vous mettez à niveau une instance.

Pare-feu

Configurez votre pare-feu pour autoriser le trafic réseau sortant du serveur MID vers votre instance et votre serveur de mise à niveau automatique.

Pour configurer votre pare-feu, utilisez les exemples de syntaxe suivants :

- `<source IP> VERS <instance_name>.service-now.com SUR LE PORT 443`
- `<source IP> VERS install.service-now.com SUR LE PORT 443`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administrer et gérer

Cette section décrit les pratiques et les directives de sécurité pour l'administration et la gestion du serveur MID dans votre environnement.

Créer un compte avec un rôle mid_server

Créez un compte d'utilisateur dans l'instance qui contient un rôle mid_server.

Lorsque vous créez un compte utilisateur, suivez ces directives :

- N'utilisez pas de compte administrateur dans l'instance pour le serveur MID.
- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte de Serveur MID.
- Le mot de passe doit comporter au moins 12 caractères avec des caractères majuscules, minuscules, numériques et spéciaux.
- Utilisez différents comptes de Serveur MID avec des mots de passe uniques pour différents serveurs MID dans une instance.
- Utilisez la fonctionnalité de sécurité SOAP stricte pour protéger toutes les tables avec des listes de contrôle d'accès (ACL) en activant *`Enforce strict security on incoming SOAP requests`* **Propriétés système** > **Services Web**.
- Modifiez les mots de passe du serveur MID à une fréquence qui correspond à la politique de mot de passe de votre organisation.

Remarque :
Pour plus d'informations, consultez Créer l'utilisateur de Serveur MID et accorder le rôle .

Configuration d'un Serveur MID sur un hôte Windows

Lorsque vous installez le serveur MID sur un hôte Windows, un service Windows est créé. Par défaut, ce service s'exécute en tant que compte système Windows local. Une fois l'installation terminée, remplacez le service Windows nouvellement créé par un compte avec le moins de privilèges requis pour exécuter le serveur MID sur l'hôte Windows.

1. Accédez à la **Gestion des ordinateurs** > **Services et applications** > **Services**.
2. Cliquez avec le bouton droit sur **Serveur MID ServiceNow**, puis sur **Propriétés**.
3. Cliquez sur l'onglet **Connexion** dans la fenêtre contextuelle.
4. Cliquez sur la case d'option en regard de **Ce compte**.
5. Entrez le nom d'utilisateur et le mot de passe appropriés du compte sous lequel le service doit s'exécuter.
6. Cliquez sur **OK**.
7. Dans la fenêtre Services, cliquez avec le bouton droit sur **Serveur MID ServiceNow**, puis cliquez sur **Redémarrer**.
8. Assurez-vous que le Serveur MID a pu redémarrer et se connecter à l'instance.

Informations d'identification Windows Discovery et Orchestration

Configurez un compte Windows ou Active Directory local sur les systèmes cibles avec le moins de privilèges nécessaire. Il n'est peut-être pas nécessaire d'utiliser les informations d'identification de l'administrateur du domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les pages de documentation produit suivantes fournissent des conseils sur le type de compte à utiliser et les autorisations requises.

- Informations d'identification Windows
- Sondes Windows et autorisations
- Microsoft Just Enough Administration (JEA) pour Discovery

Informations d'identification Linux Discovery et Orchestration

Utilisez un compte non racine avec des privilèges sudo limités sur les systèmes Linux cibles lors de la découverte et de l'orchestration.

Utilisez les directives suivantes :

- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte Linux. Le mot de passe doit comporter au moins 12 caractères avec des caractères majuscules, minuscules, numériques et spéciaux.
- Lors de la configuration des autorisations sudo, les chemins locaux vers les fichiers exécutables binaires peuvent différer selon la distribution Linux que vous exécutez, voir Commandes privilégiées du serveur MID .

Chiffrer les informations d'identification de connexion au serveur MID

Par défaut, les informations d'identification de connexion au serveur MID sont chiffrées dans le fichier config.xml.

Lors de la modification du fichier config.xml et de la fourniture du mot de passe, assurez-vous que l'attribut `encrypt="true »` existe, à l'aide de la syntaxe suivante :

```
<nom de paramètre="MID.instance.nom d'utilisateur » value="MIDsrvadmin » />
```

```
<nom de paramètre="MID.instance.password » secure="true » value="$ECUREpassw 0rd"/>
```

Remarque :
Le chiffrement des informations d'identification de connexion au serveur MID ne remplace pas un hôte de serveur non sécurisé par une mauvaise sécurité physique et réseau. Le mot de passe stocké dans le fichier config.xml est chiffré au premier démarrage du Serveur MID ou, s'il s'agit d'un Serveur MID existant, au redémarrage.

Définir la taille minimale du groupe DH sur 2 048 bits

Le National Standard Institute of Technology (NIST) a interdit l'utilisation de la clé Diffie-Hellman (DH) 1024 bits après l'année 2013. Définissez plutôt la taille minimale du groupe DH sur 2 048 bits.

1. Dans l'instance, accédez à **Serveur MID** > **Serveurs**.
2. Cliquez sur le nom du Serveur MID sur lequel vous souhaitez désactiver cette fonctionnalité.
3. Dans la configuration de Serveur MID, cliquez sur le bouton **Nouveau** en regard de Paramètres de configuration.
4. Dans le paramètre Configuration de Serveur MID, configurez les paramètres suivants :
   - **Nom de paramètre** `mid.ssh.dh_group_length_min`
   - **Valeur** `2048`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le SSL sortant

Vous pouvez désactiver SSLv2 et SSLv3 dans l'.ServiceNow AI Platform La définition de cette propriété force le serveur MID à utiliser TLS, en tirant parti de sa sécurité accrue, lors des connexions sortantes, telles que des demandes REST et SOAP.

1. Dans l'instance, accédez à **Serveur MID** > **Propriétés**.
2. Ajoutez un paramètre de configuration et définissez sa valeur comme suit :
   - **Nom** : glide.outbound.sslv3.disabled
   - **Valeur** true

Important :
La valeur de cette propriété est un remplacement sûr et ne peut pas être modifiée une fois modifiée.

Désactiver les algorithmes plus faibles

Vous pouvez désactiver les algorithmes les plus faibles afin que les requêtes à tout serveur HTTP non compatible TLS 1.2 échouent là où elles fonctionnaient auparavant.

Modifiez le fichier jre/lib/security/java.security dans le dossier de l'agent à l'aide de la syntaxe suivante :

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [autres algos faibles...]
```

Remarque :
Gardez à l'esprit que ce fichier est écrasé lors de la mise à niveau, vous devriez donc avoir un processus en place pour mettre à jour ce fichier après chaque mise à niveau.

Les utilisateurs Powershell doivent consulter l'aide de leur Windows administrateur pour désactiver les versions antérieures de TLS. Pour obtenir des détails sur les versions de TLS utilisées dans PowerShell, utilisez la commande [enum] ::GetNames([Net.SecurityProtocolType]).

Comportement réversible

Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».

Remplacement sécurisé

Les valeurs de ces propriétés ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles).

Remarque :
Les administrateurs ne sont pas en mesure de renommer ou de supprimer la propriété Remplacement sûr.

Attribut	Catégorie
Refuser par défaut en cas d'ACL vides [Mis à jour dans Centre de sécurité 1.3]	Contrôle d'accès
Exiger la vérification de l'ACL AJAXGlideRecord [Mis à jour dans Centre de sécurité 1.3]	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Catégorie
Exiger l’authentification par défaut pour les includes de script appelables par le client [Mis à jour dans Centre de sécurité 1.3]	Contrôle d'accès
Remplacement du mode de collecte (obsolète)	Propriétés de sécurité déconseillées

Aucun remplacement de base de données

Les valeurs existantes de ces propriétés ne peuvent pas être modifiées ou remplacées.

Attribut	Catégorie
Restreindre les types de fichiers téléchargeables dans le contenu statique [Mis à jour dans Centre de sécurité 1.3]	Pièces jointes

Propriétés de sécurité déconseillées

Ces propriétés de sécurité ont été déconseillées dans les versions précédentes.

Remplacement du mode de collecte (obsolète)

La `glide.whitelist.manager.collection_mode.override` propriété a été conçue pour fournir une rétrocompatibilité pour les instances hautement personnalisées. Il utilisait des appels de package qui ont été créés sur une version antérieure à Calgary et qui ont depuis été déconseillés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.whitelist.manager.collection_mode.override`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l’instance	Non
Objectif	La désactivation de la propriété Mode de collecte comble la faille de sécurité qui existe lors de l’importation d’appels de packages Java dans une instance.
Valeur recommandée	Faux
Impact fonctionnel	(Faible) Il ne devrait pas y avoir d’impact tant que les résultats de la section 10.6 sont examinés et approuvés. Pour garantir le bon fonctionnement de l’instance, testez les changements dans un environnement de non-production avant le déploiement dans l’environnement de production
Risque de sécurité	Les appels d’API côté client (élevés) qui entraînent la récupération de données ou l’accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Validez-les pour l’autorisation et la restriction de l’accès aux objets sensibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification SMTP (obsolète)

Propriété *glide.smtp.auth* désignée si un serveur SMTP doit exiger des entrées d'authentification par nom d'utilisateur et mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	glide.smtp.auth
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Applique l'authentification SMTP
Valeur recommandée	vrai
Impact fonctionnel	(Élevé) Cette correction applique l'authentification au serveur de messagerie externe avant que le contenu ne soit livré sous la forme d'un e-mail. Si l'automatisation est configurée pour fournir du contenu d'e-mail, il peut y avoir un impact tant que vous n'avez pas défini la propriété et fourni un nom d'utilisateur/mot de passe pertinent pour l'accès au serveur de messagerie.
Risque de sécurité	(Faible) Activez l'authentification SMTP avant d'envoyer le contenu au serveur de messagerie externe. L'authentification doit toujours avoir lieu avant que les transactions n'aient lieu vers/depuis l'instance.
Références	Propriétés d'e-mail

Utilisation de JavaScript Contrôle d'accès au contenu

Si vous êtes un client mis à niveau, vous pouvez utiliser le contrôle d'accès au contenu JavaScript pour modifier la liste des URL JavaScript tierces bloquées dans votre instance.

Avant de commencer

Si vous êtes un client mis à niveau, vous disposez d'un accès en lecture et en écriture à la table.

Si vous êtes un nouveau client, tous les enregistrements sont masqués. Contactez le ServiceNow® support pour obtenir de l'aide.

Rôle requis : admin

Procédure

1. Dans le navigateur d'application, recherchez sys_js_content_provider_rule.list.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle du fournisseur de contenu JavaScript

Champ	Description
Actif	Option qui, lorsqu'elle est sélectionnée, rend la règle active. Si aucune autre règle ne correspond, si aucune autre règle ne correspond, l'URL du **chemin d'accès** est admise.
Chemin d'accès	URL absolue d'un fichier JavaScript. **Remarque :** Chaque chemin a quatre variantes. Par exemple, le chemin d'accès `/scripts/lib/jquery/jquery-1.8.2.min.js` bloque les URL suivantes : ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.jsx
Action	Option pour ○ **Refuser** : le serveur renvoie une réponse **404 Introuvable** pour l'URL du **chemin d'accès** ou l'une de ses variantes. ○ **Autoriser** : le serveur renvoie le contenu du fichier pour l'URL du **chemin d'accès** ou l'une de ses variantes. ○ **Redirection** : le serveur renvoie le contenu d'un fichier alternatif tel que spécifié dans le champ Chemin de redirection.
Application	Option qui spécifie le champ d'application de la règle. **Global** est la valeur par défaut. **Remarque :** Cette fonctionnalité ne dépend pas du champ d'application/de l'application ou du domaine.
Chemin de redirection	Champ qui clarifie le chemin vers lequel effectuer la redirection. Lorsque **l'action** est définie sur **Rediriger**, une demande d'URL de chemin d'accès reçoit le contenu de cette URL à la place.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autres ressources de sécurisation renforcée de la sécurité

Voici d'autres sources d'informations sur le renforcement des contrôles de sécurité, en ce qui concerne le ServiceNow AI Platform.

Ressource	Description
Portail de test de sécurité	Portefeuille de services de sécurité sur HI
KB0538598	Test de pénétration de l'application client | Politique et procédure
KB0546756	Désactiver l'accès public au système de gestion de contenu (CMS)
KB0550071	ServiceNow, Inc. Examen du contrôle d'accès à l'instance
KB0550613	Identification et activation des restrictions d'adresse IP
KB0550828	Auditer et examiner les transactions GlideAjax
KB0550837	Rattrapage du sandboxing de script
KB0551031	Rattrapage de sécurité pour l'interface utilisateur de réinitialisation du mot de passe
KB0552835	Rattrapage pour les comptes d'utilisateurs de démonstration
KB0529232	ServiceNow, Inc. Surveillance : vue d'ensemble et aperçu
KB0564232	Utilisation de l'application ServiceNow, Inc. mobile avec authentification externe
Sécurité et risque	ServiceNow, Inc. Communauté

Traduction automatique

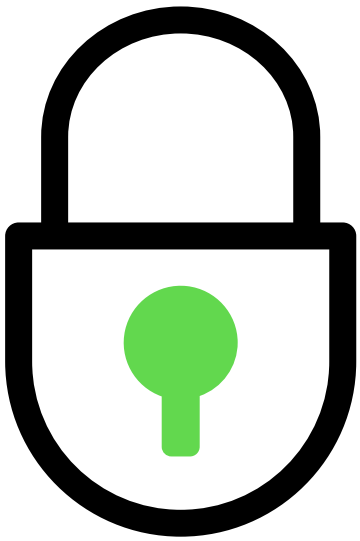
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confidentialité de la plateforme

La confidentialité vous permet de masquer la date sensible sur l'instance.

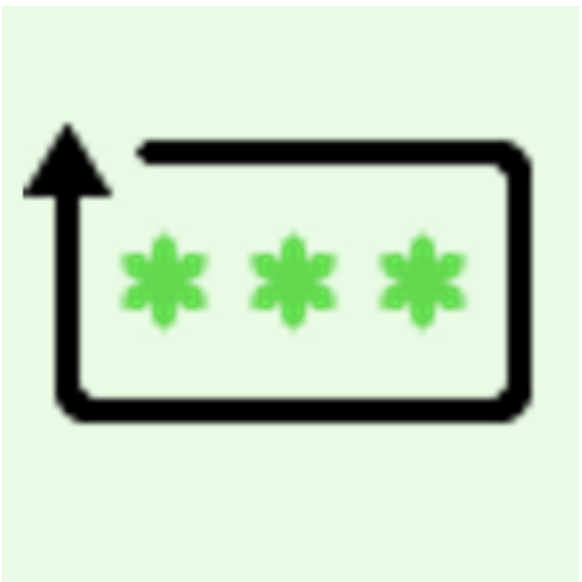
Applications du magasin

Confidentialité des données



Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production.

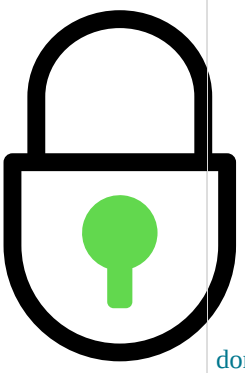
Découverte de données



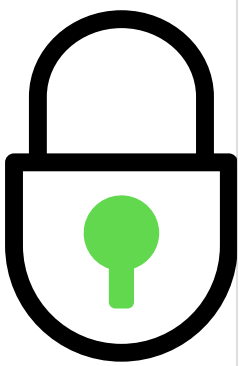
Utilisez la détection de données pour identifier les données sensibles au sein d'une instance afin de classer, protéger ou générer des rapports.

Modules d'extension

Confidentialité des données (classique)

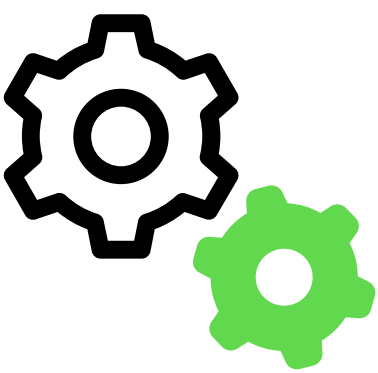


Anonymisation des données



L'anonymisation des données permet de

Classification des données



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le module d'extension Confidentialité des données (classique) hérité.	transformer facilement les données afin qu'elles ne soient pas identifiables et de les rendre plus conformes à la réglementation en matière de confidentialité des données.	Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Exploration de la confidentialité des données

Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production. Une fois anonymisées, les données utilisateur ne sont plus considérées comme des informations privées réglementées.

Explique l'importance de la confidentialité des données et les mesures que les entreprises peuvent prendre pour protéger les informations sensibles par la classification et l'anonymisation. À l'aide de l'application Data Privacy Store, nous donnons un aperçu du tableau de bord principal et des options.

Les développeurs doivent utiliser des données sur des instances de non-production pour s'assurer que leurs implémentations fonctionnent comme prévu. Bien que l'importation de données à partir de votre instance de production soit un moyen utile de simuler la production, elle présente un risque de sécurité. Les administrateurs peuvent utiliser la confidentialité des données pour fournir aux développeurs des données qui ne contiennent pas d'informations privées afin de travailler en toute sécurité dans un environnement de non-production.

Classification des données

Identifiez et classez vos données sensibles selon des critères prédéfinis déterminés par le niveau de sensibilité des types de données de votre instance. Les niveaux de sensibilité des données permettent de déterminer comment chaque type de données classifiées doit être traité. Plusieurs classes prédéfinies sont fournies avec la confidentialité des données de niveau de base. Utilisez la section de classification de Confidentialité des données pour étiqueter et regrouper les données au sein de votre instance. Ajoutez des classes, affichez la structure de classe de données et classez les données. Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur.

Explique comment classer des données à l'aide de l'application du magasin Confidentialité des données.

Anonymisation des données utilisateur

En tant qu'administrateur, vous définissez s'il faut anonymiser toutes les informations pour tous les utilisateurs ou pour un sous-ensemble d'utilisateurs. Lorsqu'elles sont anonymisées, les données des enregistrements des utilisateurs sélectionnés sont remplacées par des valeurs randomisées ou des valeurs que vous définissez. Lors du remplacement des valeurs, il est possible de conserver la structure des données à l'aide de diverses techniques.

Explique comment anonymiser des données à l'aide de l'application du magasin Confidentialité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confidentialité des données

Permet Confidentialité des données de classer les données sensibles et de supprimer les informations personnelles identifiables (PII) des données utilisateur dans une instance de production et d'anonymiser les données dans les instances de non-production.

Remarque :
Vous pouvez également utiliser le module d'extension Confidentialité des données (classique) hérité .

Détails de l'installation

Les applications suivantes doivent être installées sur votre instance :

- Confidentialité des données (classique) [com.glide.data_privacy]
- Confidentialité des données [sn_dp_store_app]
- Découverte de données [sn_data_discovery]
- API de découverte de données[com.glide.data_discovery]

Voici comment fonctionne l'installation :

- L'installation de l'application Data Privacy Store installe automatiquement l'application Data Discovery Store, le module d'extension Data Privacy (Classic) et le module d'extension Data Classification.
- L'installation de l'application de stockage de découverte de données installera automatiquement le module d'extension API de découverte de données

Considérations

- Seules les données classifiées peuvent être anonymisées. Pour plus d'informations sur les classes de données et la classification, consultez Classification des données (classique) ou Classification des données App Store.
- Les PII dans les journaux et autres données d'audit ne sont pas anonymisées.
- Seules les données structurées peuvent être anonymisées. Les données non structurées, telles que les champs journal, les commentaires, les pièces jointes et d'autres champs dans lesquels du texte partiel peut représenter des informations personnelles ne sont pas anonymisées. Consultez Types de champs pris en charge pour l'anonymisation pour plus d'informations.
- Les intégrations avec les systèmes d'authentification unique (SSO) peuvent resynchroniser les informations des utilisateurs à partir de leurs systèmes de source de vérité. Il n'y a pas de mécanisme en place pour assurer la permanence de la désidentification des données sys_user. Pour plus d'informations sur l'administration et les sys_users utilisateurs, voir Administration utilisateur .

Confidentialité des données

Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrir Confidentialité des données



En savoir plus sur la confidentialité des données.

Configurer Confidentialité des données



Découvrez comment configurer la confidentialité des données.

Rôles dans Confidentialité des données



Obtenez des détails sur les rôles dans Confidentialité des données.

Fonctionnalités avancées de confidentialité des données



Découvrez les fonctionnalités avancées de la confidentialité des données.

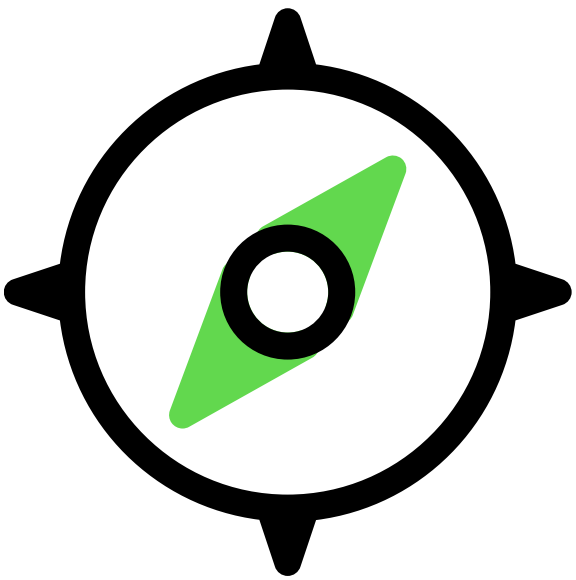
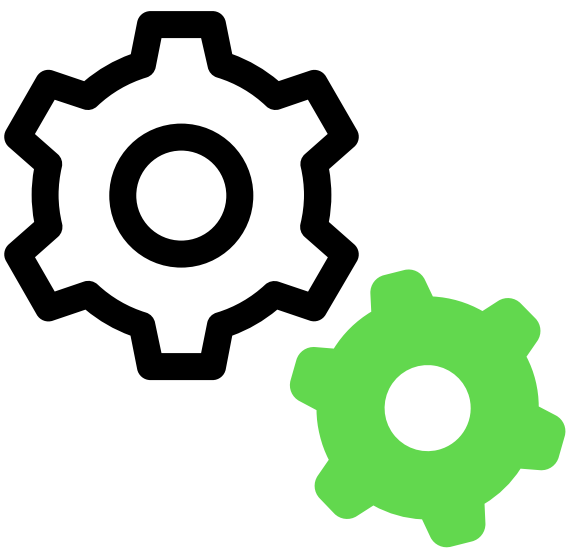
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confidentialité des données pour Now Assist

Définissez et configurez la façon de détecter et d'anonymiser les données sensibles à partir des invites de l'IA générative.

Premiers pas

Explorer	Configurer
	
En savoir plus sur la confidentialité des données pour Now Assist	Configurer Confidentialité des données pour Now Assist

Remarque :
Confidentialité des données pour Now Assist détecte et masque les données sensibles en fonction des schémas Regex et ne prend pas en charge les schémas de données contextuelles (type modèle).

Explorer Confidentialité des données for Now Assist

En savoir plus sur Now Assist la façon d'améliorer Confidentialité des données votre capacité à protéger les données sensibles.

Confidentialité des données pour Now Assist obtenir une vue d'ensemble

Les données sensibles telles que l'âge, le numéro de téléphone et d'autres informations personnellement identifiables (PII) peuvent être masquées afin qu'elles ne soient pas traitées par les invites de l'IA générative. Le texte d'espace réservé et les données anonymisées sont envoyés avec l'invite à la place, et ces valeurs sont remplacées par le texte d'origine après réception de la réponse du module d'apprentissage des langues volumineux (LLM). Ce masquage bidirectionnel garantit que les utilisateurs finaux reçoivent des réponses précises, mais que les données sensibles ne sont pas exposées au LLM.

Il y a quelques considérations à prendre en compte lors de la configuration Confidentialité des données de Now Assist. Consultez Configurer Confidentialité des données pour Now Assist pour connaître les détails de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

Confidentialité des données pour Now Assist détecte et masque les données sensibles en fonction des schémas Regex et ne prend pas en charge les schémas de données contextuelles (type modèle)

Configurer Confidentialité des données pour Now Assist

Configurez une configuration avancée de confidentialité des données pour anonymiser les informations personnellement identifiables (PII) dans les applications d'IA générative.

Avant de commencer

Les applications suivantes doivent être installées sur votre instance :

- Confidentialité des données (Classique) [com.glide.data_privacy]
- Confidentialité des données [sn_dp_store_app]
- Détection de données [sn_data_discovery]
- Détection de données API[com.glide.data_discovery]

L'installation de la dernière version du contrôleur d'IA générative installera automatiquement l'application du magasin de confidentialité des données (sn_dp_store_app). L'application du magasin Confidentialité des données installe automatiquement l'application du magasin Découverte de données[sn_data_discovery], le module d'extension Confidentialité des données (classique)(com.glide.data_privacy) et les Détection de données API[com.glide.data_discovery].

Rôle requis : now_assist_data_privacy_admin

Important :

Vous n'avez pas besoin d'une licence active complète pour configurer Confidentialité des donnéesNow Assist le fichier .

Procédure

1. Accédez à la **Tous** > **Confidentialité des données (classique)** > **Configuration de la politique de confidentialité avancée**.
   Si vous avez précédemment utilisé le gestionnaire de données sensibles pour faciliter la désidentification des données pour l'IA générative, vous pouvez déjà voir une politique de confidentialité configurée. Vos expressions régulières précédemment configurées ont été migrées dans le cadre de votre mise à niveau. Si vous avez déjà une politique de données pour Now Assist, passez à l'étape 6.
2. Sélectionnez **Nouveau**.
3. Entrez un nom pour la politique de confidentialité.
4. Dans le champ **Canal de données** , sélectionnez le canal de données à utiliser.
5. Définir **Actif** sur vrai, puis sélectionner **Soumettre** pour créer la configuration avancée de la politique.
   Une seule configuration de politique pour chaque canal de données peut être active à la fois. Pour activer une nouvelle configuration de politique avancée, vous devez définir **Actif** sur false pour toutes les autres configurations de politique sur ce canal de données.
6. Une fois que vous êtes redirigé vers la liste des configurations avancées de stratégie, ouvrez l'enregistrement que vous avez créé.
   Ouvrez l'enregistrement existant avec le canal de données Now Assist, le cas échéant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour ajouter un schéma de données à désidentifier, sélectionnez **Sélectionner des schémas de données**.
8. **Facultatif :** Pour créer votre propre modèle de données, reportez-vous à la section Configurer des Détection de données schémas.
9. Sélectionnez vos schémas de données, puis sélectionnez **Enregistrer**.

Résultats

Les données interceptées par les expressions régulières sélectionnées dans les schémas de données sont anonymisées pour les applications d'IA générative. Dans cet exemple de stratégie, elle est configurée pour intercepter une série de schémas de données actifs, puis utiliser le canal de données d'extraction de données.

Confidentialité des données

L'application de stockage de la confidentialité des données est une actualisation Next Experience pour la classification et la confidentialité des données avec une apparence et une convivialité modernes. L'application du magasin de confidentialité des données est prise en charge dans Utah et les versions ultérieures.

La confidentialité des données est composée de plusieurs composants : vue d'ensemble, classification et anonymisation.

Vue d'ensemble

Utilisez la section Vue d'ensemble comme point de départ pour gérer votre conformité en matière de données et de confidentialité des données. Consultez Vue d'ensemble de la confidentialité des données pour en savoir plus.

Classification

La classification des données est le processus d'organisation des données en catégories qui facilitent leur récupération, leur tri et leur stockage pour une utilisation ultérieure. L'utilisation d'un système de classification permet de se concentrer sur les exigences de la politique de confidentialité et de sécurité. Classez les données à utiliser pour l'anonymisation. Pour plus d'informations sur les classes de données et la classification, reportez-vous à la section Classification des données.

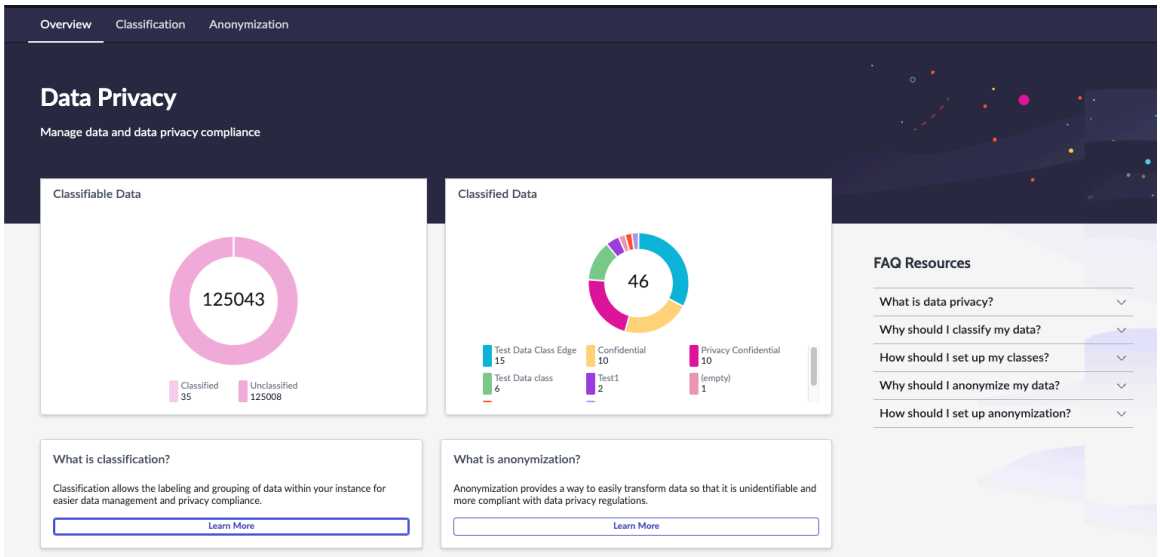
Vue d'ensemble de la confidentialité des données

La page d'accueil Vue d'ensemble est un point de départ pour gérer la conformité de vos données et de la confidentialité des données.

Le tableau de bord Vue d'ensemble présente l'état actuel des classifications de données et des tâches d'anonymisation au sein de votre instance. Vous pouvez afficher vos données avec le tableau de bord Vue d'ensemble pour voir la quantité de données pouvant être classées, les classes de données disponibles, la quantité de données dans chaque classe et l'état général des tâches d'anonymisation. Les données classifiées sont divisées en différentes catégories. La sélection d'une sous-catégorie dans l'un ou l'autre des graphiques ajoutera ou supprimera la catégorie du graphique global et ajustera les nombres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Données classifiables

Affiche le nombre total d'enregistrements de données dans l'instance qui peuvent être classifiés. Ce nombre est ventilé entre le nombre total de données classifiées et le nombre total de données non classifiées. Cela donne aux administrateurs un aperçu rapide des opportunités de classification potentielles.

Données classifiées

Affiche le nombre total d'enregistrements de données dans l'instance qui ont été classifiés. Le nombre est décomposé en nombre total de données classifiées pour chaque classe de données affectée. Cela permet de comprendre rapidement la quantité de données qui ont été classées dans chaque zone.

Tâches d'anonymisation

Affiche les tâches de confidentialité des données actuellement en cours de traitement des tâches terminées sur votre instance de non-production pour les tâches d'utilisateur et de classe de données.

En savoir plus

Les sections **En savoir plus** fournissent un aperçu rapide de la compréhension de la classification et de l'anonymisation, ainsi qu'un moyen facile de commencer dans le processus.

Ressources de la FAQ

Accédez aux ressources d'apprentissage du produit sur la classification ou l'anonymisation pour obtenir des informations supplémentaires sur la façon de commencer à sécuriser votre instance avec la confidentialité des données.

Classification des données

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Classification des données Active la prise en charge de :

- Visibilité des types de données hébergées sur une ServiceNow AI Platform instance.
- Respect des lois sur la protection de la vie privée et respect des exigences réglementaires pour les secteurs tels que les services financiers et la fabrication de dispositifs médicaux.

Classifications des données

La classification des données est un processus autonome dans lequel vous appliquez manuellement des classifications de données à des entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous classez les données selon ce que vous jugez approprié pour votre entreprise et vous pouvez modifier les classes de données disponibles si nécessaire.
- Lorsque vous classez des données, vous pouvez utiliser les classifications de données prédéfinies ou créer les vôtres. Bien que l'utilisation de classifications de données prédéfinies soit facultative, il est conseillé de le faire comme point de départ. Ces classifications de données prédéfinies sont incluses dans les données de démonstration que vous pouvez installer dans votre instance.
- Si vous créez vos propres classifications de données, vous pouvez également concevoir un système hiérarchique hiérarchisé avec des classifications de données parentes et enfants.

Remarque :
Classification des données prend en charge Séparation de domaine et la table data_classification elle-même est séparée par processus. Consultez Séparation de domaine et Classification des données pour plus d'informations.

Cas d'utilisation

Le Règlement général sur la protection des données (RGPD) est un règlement de l'Union européenne dont l'objectif est de permettre aux individus de contrôler leurs propres données personnelles. Vous pouvez utiliser des classifications de données, telles que les informations personnellement identifiables, pour identifier où les données personnelles sont stockées dans votre instance. En appliquant les mécanismes de sécurité appropriés pour protéger ces données personnelles contre les fuites, votre organisation répond aux exigences du RGPD.

Si vous stockez des informations sur les clients dans le , utilisez le code de classification des informations personnellement identifiables (PII) lorsque cela est nécessaire pour suivre les données soumises à la réglementation des lois locales sur la ServiceNow AI Platform confidentialité.

Vous pouvez appliquer une classification de données restreinte aux colonnes de la table Employé qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (NSS). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté les classifications de données aux bonnes colonnes. Ils peuvent également afficher les détails de classification pour les types d'informations restreints.

Créer des classifications des données

Créez vos propres classifications de données définies par l'utilisateur dans la table [data_classification] que vous pouvez ensuite affecter à des colonnes spécifiques dans des tables spécifiques. Créez de nouvelles classes de données pour démarrer le processus de classification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : data_classification_admin, admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Confidentialité des données** > **Classification**.
2. Sélectionnez **+Ajouter une classe de données**.

   Remarque :
   Plusieurs classes de données sont incluses dans le système de base.

3. Renseignez les champs du formulaire.

Champ	Description
Nom de classe	Nom de la classification des données.
Classe parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas un enfant d'une classification de données parente.
Description	Description de la classification des données.

4. Cliquez sur **Envoyer**.
   La nouvelle classe de données est ajoutée. Si la classe de données est un enfant, elle sera répertoriée sous le parent dans la barre de navigation de gauche.

Classifier des données

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Affectez des classifications de données à des colonnes de table spécifiques dans la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, cela crée des entrées dans la table Classe de données de dictionnaire [m2m_dictionary_dataclass], que vous pouvez ensuite passer en revue dans le tableau de bord Vue d'ensemble.

Avant de commencer
Rôle requis : data_classification_admin, admin

Procédure

1. Sélectionnez **Nouveau** pour affecter les données d'une table à classer.
2. Sélectionnez la classe de données dans la liste déroulante.
3. Sélectionnez les enregistrements reflétant les tables et les colonnes à classer.
   Choisissez des lignes supplémentaires à afficher par page dans le tableau pour simplifier la localisation d'un tableau particulier.
4. Sélectionnez **Classifier les données**.
   Les données sont classées sous le nom de classification dans la table de données classifiées.
5. Affichez ou exportez les données au format Excel, CSV, JSON ou PDF.
   Choisissez de télécharger les données dans le format choisi ou de les recevoir par e-mail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Anonymisation des données

L'anonymisation permet de transformer facilement les données afin qu'elles ne soient pas identifiables et de les rendre plus conformes à la réglementation en matière de confidentialité des données.

Les administrateurs peuvent effectuer le processus d'anonymisation dans les instances de production et de non-production. La confidentialité des données peut être utilisée dans les instances de production pour désidentifier les utilisateurs. L'anonymisation des classes de données ne doit être utilisée qu'avec des instances de non-production. Cette conservation garantit que certaines données, telles que les adresses e-mail ou les adresses physiques, sont remplacées par des versions au format similaire, mais anonymisées.

Les administrateurs peuvent également utiliser l'anonymisation dans le cadre de leurs processus de droit à l'oubli (RTBF) du Règlement général sur la protection des données (RGPD) pour anonymiser les informations des utilisateurs. Consultez https://gdpr-info.eu/art-17-gdpr/ pour plus d'informations.

Utilisez la section d'anonymisation de Confidentialité des données pour créer et afficher des politiques et des techniques de confidentialité, et pour effectuer l'affectation de confidentialité en bloc. Affichez toutes les tâches, avec la description, la politique privée utilisée et l'état. Pour accéder à la section d'anonymisation, un administrateur doit d'abord accéder aux rôles data_privacy_admin et data_privacy_processor.

Techniques d'anonymisation

Les techniques d'anonymisation sont des options que vous sélectionnez pour déterminer le mode d'anonymisation de vos données. Vous devez créer une technique d'anonymisation à référencer dans la tâche d'anonymisation. Voir Créer des techniques d'anonymisation pour associer une technique de confidentialité à une **configuration de technique d'anonymisation** associée.

Politiques d'anonymisation

Configurez une politique d'anonymisation pour spécifier les techniques de confidentialité des données utilisées lors de l'anonymisation de vos données. Consultez la section pour Créer des politiques d'anonymisation en savoir plus.

Tâches d'anonymisation

Les tâches d'anonymisation utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces emplois, reportez-vous à Créer une tâche d'anonymisation.

Créer des techniques d'anonymisation

Créez une configuration de technique de confidentialité des données pour personnaliser la façon dont la confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et administrateur

Procédure

1. Accéder au rôle **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Sélectionnez **Afficher les techniques**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Plusieurs techniques prédéfinies sont disponibles pour la sélection.

Technique	Description
Remplacement sélectif	Cette technique remplace sélectivement les données de chaîne. Tous les caractères entre les index de début et de fin de l'entrée sont remplacés par le caractère que vous choisissez. Vous pouvez spécifier des caractères à exclure du masquage : ◦ start_index : la technique masque les données commençant par le caractère spécifié. S'il est laissé vide, le masquage commence par le premier caractère. ◦ end_index : la technique masque les données du début de la chaîne jusqu'au caractère spécifié. Si ce champ est laissé vide, le masquage se termine au dernier caractère. ◦ exclude_char : définissez un caractère à exclure du masquage. ◦ replacement_char : Définissez un caractère utilisé pour le masquage. Si aucun n'est fourni, les astérisque (*) sont utilisés par défaut.
Remplacement statique	Cette technique échange les valeurs avec des valeurs statiques. Les données chaîne, numéro et date peuvent utiliser cette technique : ◦ date_time_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss. ◦ date_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj. ◦ number_value : remplacez les valeurs de nombres par ce nombre. ◦ string_value : remplacez les valeurs de chaîne par ce texte. ◦ number_type : accepte un nombre entier
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de façon aléatoire. Les données chaîne et numéro peuvent utiliser cette technique.
Supprimer	Cette technique supprime les valeurs et les remplace par des valeurs vides (null).
Aucune action	Cette technique est un espace réservé. Il ne modifie pas les champs lorsqu'ils sont sélectionnés.
Remplacement sélectif par X	Transforme les données de chaîne et remplace sélectivement les caractères sensibles par la lettre X. **Remarque :** Technique par défaut pour les schémas de données dans Exploration Détection de données (classique).
Anonymisation du modèle de données	Anonymise uniquement les schémas de données découverts dans des champs de données non structurés tout en conservant intact le contexte sous-jacent. **Remarque :** Paramètres de cette technique pour les paramètres de la technique d'anonymisation des modèles de données de référence dans Exploration Détection de données (classique).

4. Sélectionnez **Ajouter une technique personnalisée**, si vous n'utilisez pas une technique prédéfinie.
5. Renseignez les champs du formulaire Personnaliser la **technique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ 1	Description
Technique de base	Sélectionnez une technique prédéfinie, car les techniques personnalisées sont basées sur les techniques prédéfinies.
Nom de la technique	Entrez un nom pour la technique.
Description de la technique	Entrez une description de la technique.

6. Sélectionnez **Suivant**.
7. Entrez les paramètres de la technique.
   Les valeurs paramétrées disponibles dépendent de la technique de confidentialité que vous avez sélectionnée. Il n'existe aucune valeur paramétrée pour les techniques **Aucune action** et **Supprimer** .

Valeurs paramétrées de confidentialité pour les techniques de base

Technique de base	Valeur du paramètre de la technique de confidentialité	Description	Valeur par défaut
Remplacement sélectif	end_index	La technique masque les données du début de la chaîne jusqu'au caractère spécifié. S'il est laissé vide, le masquage se termine au dernier caractère.	(Vide)
Remplacement sélectif	exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plusieurs caractères sont saisis, le premier caractère est utilisé.	(Vide)
Remplacement sélectif	replacement_char	Caractère à utiliser lors du remplacement de valeurs à l'aide d'un remplacement sélectif.	Un astérisque (*) est utilisé si aucune autre valeur n'est saisie.
Remplacement sélectif	start_index	La technique masque les données commençant par le caractère spécifié.	Si ce champ est laissé vide, le masquage commence au premier caractère.
Remplacement statique	date_time_value	Remplacez les valeurs de date et d'heure par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss.	1988-11-11 10:10:10
Remplacement statique	date_value	Remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj.	1988-11-11

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Technique de base	Valeur du paramètre de la technique de confidentialité	Description	Valeur par défaut
Remplacement statique	number_value	Remplacez les valeurs de nombres par ce nombre.	1234567
Remplacement statique	string_value	Remplacez les valeurs de chaîne par ce texte.	TEXT123
Remplacement aléatoire	preserve_data_length	Définissez la valeur **sur vrai** pour préserver la longueur des données. Les données dé-identifiées auront la même longueur que les données d'origine.	Vrai

8. Sélectionnez **Créer une technique personnalisée**.
   Votre technique personnalisée est ajoutée aux techniques d'anonymisation.

Que faire ensuite

Consultez Créer des politiques d'anonymisation pour configurer une politique d'anonymisation afin de spécifier les techniques utilisées lors de l'anonymisation de vos données.

Créer des politiques d'anonymisation

Configurez une politique d'anonymisation pour spécifier les techniques utilisées lors de l'anonymisation de vos données.

Avant de commencer

La configuration de confidentialité des données définit les tables, les sys_user et autres, et les colonnes à désidentifier, en fonction du cas d'utilisation, et spécifie les types paramétrés des techniques à utiliser lors de la désidentification des données.

Remarque :
Pour terminer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez Créer des techniques d'anonymisation pour en savoir plus.

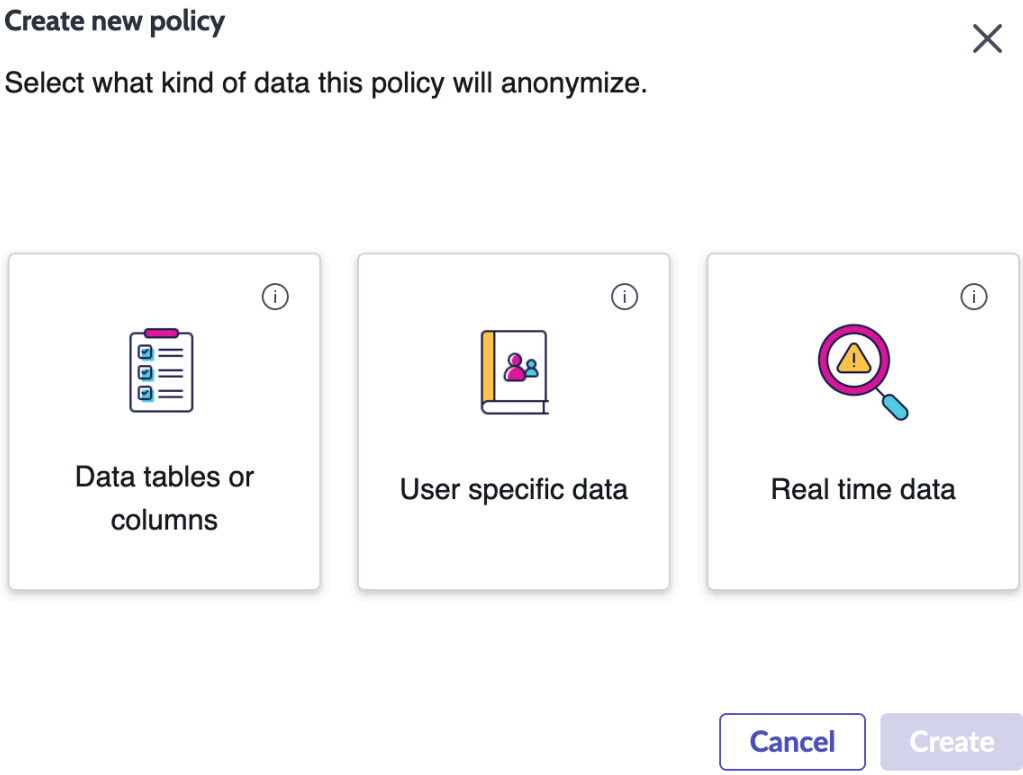
Rôle requis : data_privacy_admin et administrateur

Procédure

1. Accéder au rôle **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
   Toutes les politiques d'anonymisation s'affichent. Des politiques publiées sont disponibles pour planifier la tâche d'anonymisation.
3. Sélectionnez **Créer une nouvelle politique**.
4. Sélectionnez cette option pour anonymiser des **tables ou des colonnes de données**, des **données spécifiques à l'utilisateur** ou des **données en temps réel**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Type de données	Description
Tables ou colonnes de données	Les enregistrements qui correspondent à la politique de données sont anonymisés.
Données spécifiques à l'utilisateur	Sélectionnez un ensemble d'utilisateurs ou de groupes d'utilisateurs à anonymiser.
Données en temps réel	Anonymiser les entrées en temps réel pour un ensemble de colonnes.

Les politiques de confidentialité des données ne peuvent s'appliquer qu'aux données classifiées. Pour plus d'informations sur la classification des données, reportez-vous à Classification des données.

5. Sélectionnez **Créer**.
   Des étapes séquentielles sont requises pour compléter la politique, **définir les détails**et **affecter des techniques**. **La sélection de la référence de l'utilisateur** est également requise lors de la définition de la politique pour les données spécifiques à l'utilisateur.
6. Définissez les détails de la nouvelle politique d'anonymisation.
   - Entrez le nom de la politique dans le champ **Nom** et la description de la politique dans le champ **Description** .
   - Définir les canaux qui activent automatiquement la politique et la priorité des canaux dans **Canaux d'activation**
   - Dans le champ **Classe de données** , sélectionnez la classe de données à utiliser avec cette stratégie.
   - Activer ou désactiver l'anonymisation des données en temps réel. Reportez-vous à l'étape 8 si l'anonymisation des données en temps réel est activée.

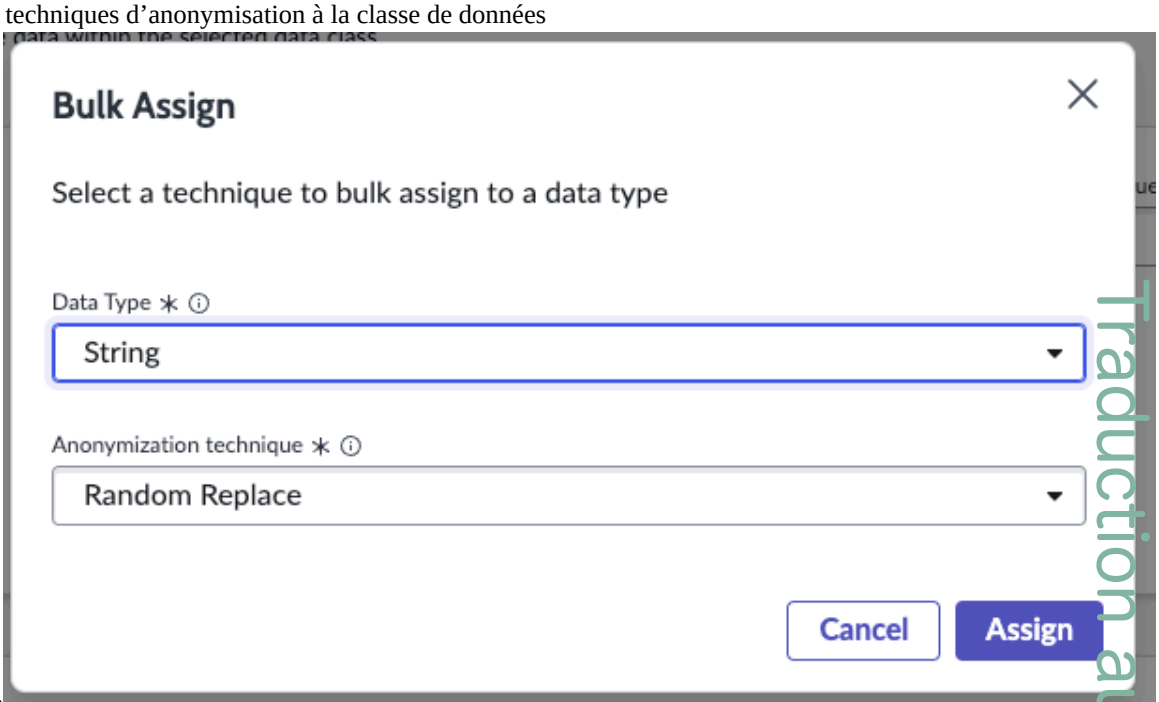
Traduction automatique

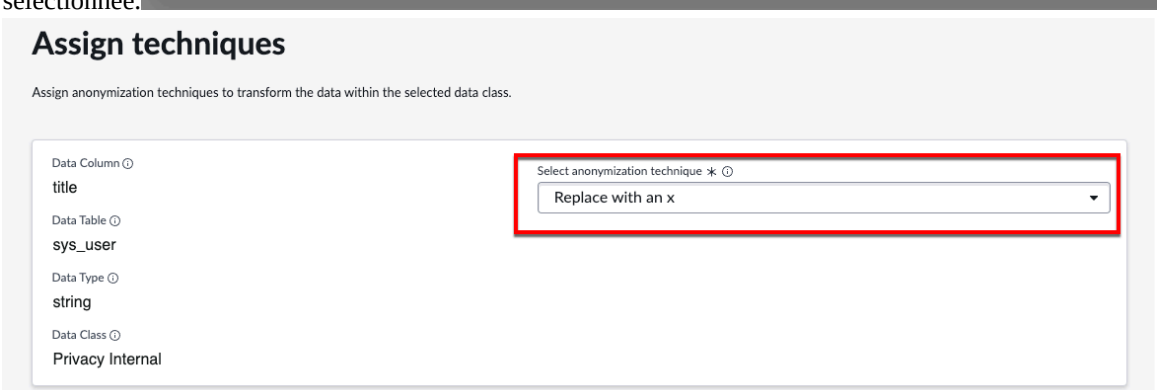
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous n'anonymisez pas une entrée, sélectionnez la technique **Ne rien faire** plutôt que de laisser l'entrée vide. Les politiques avec des valeurs vides dans le champ Configuration de la technique de confidentialité ne peuvent pas s'exécuter lorsqu'elles sont utilisées dans les tâches de confidentialité des données.

Une fois la classe de données sélectionnée, le formulaire Affecter des techniques s'affiche pour chaque enregistrement renvoyé pour la classe de données définie.

7. Affectez des techniques d'anonymisation à la classe de données sélectionnée.





8. **Facultatif :** Entrez les tables enfants à analyser.
Les tables enfants du parent sont anonymisées. Si une table n'a pas d'enfants, cette option ne sera pas disponible.

Avertissement :
Une tâche parent échouera si une tâche enfant échoue.

9. **Facultatif :** Si l'option Anonymisation du modèle de données est sélectionnée, sélectionnez la technique d'anonymisation à utiliser.
10. **Facultatif :** Définissez l'ordre des schémas de données.
11. **Facultatif :**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :
Utilisez la fonctionnalité **Test** pour tester des exemples d'entrées. Vous pouvez consulter les mesures à partir du résultat, telles que le temps d'analyse, le résultat et les schémas détectés.

Sélectionnez le bouton **Test** pour tester la politique.

12. **Important :**
Toutes les tables doivent avoir une entrée sys_dictionary correcte.

Sélectionnez **Enregistrer**.

13. Sélectionnez **Publier** pour mettre à jour la politique d'anonymisation pour la planification et revenir aux politiques d'anonymisation.

Remarque :
Seules les politiques publiées peuvent être utilisées pour la planification des tâches d'anonymisation.

Que faire ensuite
Créer une tâche d'anonymisation.

Configurer la demande de clone d'anonymisation des données

L'intégration de clone de confidentialité des données est configurée à l'aide d'un script PostClone pour créer et exécuter des tâches de confidentialité des données pour les politiques configurées sur la cible. Une fois le script exécuté, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine.

Avant de commencer
Le script PostClone de confidentialité des données est installé avec l'activation du module d'extension Confidentialité des données (sn_dp_store_app). Consultez Activer la confidentialité des données pour en savoir plus.

Rôle requis : data_privacy_clone_processor, data_privacy_admin et admin

Procédure

1. Activez le module d'extension de confidentialité des données (sn_dp_store_app) sur l'instance source.
Le script PostClone de confidentialité des données est installé.
2. Accéder au rôle **data_privacy_admin** .
Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
3. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
4. Sélectionnez **Créer une nouvelle politique**.
Consultez Créer des politiques d'anonymisation pour en savoir plus.
5. Sélectionnez **des tables ou des colonnes de données**.
6. Sélectionnez **Créer**.
7. Entrez un nom et sélectionnez une classe de données.
8. Sélectionnez cette **option pour activer la politique pendant le clonage**.
9. Sélectionnez l'ordre des politiques à exécuter s'il existe plusieurs politiques de clone.
Une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application supérieur peut commencer avant une autre tâche d'ordre inférieur, si la tâche avec l'ordre supérieur n'implique aucune table liée à une autre tâche d'ordre inférieur.
10. Sélectionnez **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Terminez la configuration de la politique et publiez-la.
12. Sauvegardez les configurations de confidentialité des données.
13. Planifiez la tâche d'anonymisation.
    Pour en savoir plus, reportez-vous à la rubrique Créer une tâche d'anonymisation.
14. En tant qu'administrateur de la confidentialité des données, soumettez une demande de clone.

Résultats

Le script PostClone de confidentialité des données s'exécute sur l'instance cible et le script PostClone crée un enregistrement de tâche fédérée de confidentialité des données sur l'instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données pour chaque politique post-clone, dans l'ordre de l'application, sur l'instance cible.La source de sauvegarde est clonée sur l'instance cible. Le script PostClone de confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l'instance cible.

Le processeur clone de confidentialité des données élevée peut se connecter à l'instance cible et surveiller l'état de la tâche fédérée post-clonage sur dp_federated_job.list et dp_job.list.

Créer une tâche d'anonymisation

Configurez une tâche de confidentialité des données sur votre instance de production pour utiliser des données rendues anonymes sur votre instance de non-production pour les tâches d'utilisateur et de classe de données.

Avant de commencer

La tâche de confidentialité des données prend en charge deux cas d'utilisation de désidentification :

- Données sensibles d'sys_users spécifiques
- Données sensibles d'une classe de données particulière.

Rôle requis : data_privacy_processor et admin

Procédure

1. Élevez-vous au rôle **data_privacy_processor** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Dans une politique d'anonymisation, sélectionnez **Planifier la tâche** pour que la politique soit utilisée dans la tâche.
   Une politique doit être à l'état Publié pour planifier une tâche d'anonymisation.

   ⚠ Avertissement :
   Les tâches d'anonymisation sont très destructrices et ne peuvent être inversées qu'en cas de restauration. Vérifiez toutes les informations, telles que les enregistrements et la table traitée, avant de planifier une tâche.

4. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs des tâches de confidentialité des données

Champ	Description
Politique utilisée	Nom en lecture seule de la configuration de politique de confidentialité sélectionnée à utiliser pour cette tâche. Modifiez la politique pour afficher des informations supplémentaires sur la politique. Pour en savoir plus sur les configurations de la politique de confidentialité, reportez-vous à la section Créer des politiques d'anonymisation.
Description de poste	Description de la tâche.
Heure de début	Début de l'heure d'exécution de cette tâche dans **HH :MM :SS.**
Heure de fin	La fin de la fenêtre de temps pour exécuter cette tâche dans **HH :MM :SS.** L'heure de fin doit être postérieure à l'heure de début. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, elle sera mise en pause et reprendra au début de la fenêtre d'heure suivante.
Essai	Exécutez la tâche comme un test. Aucun enregistrement n'est affecté lors de l'exécution de cette tâche. Les résultats sont affichés dans la liste **des tâches** , comme si la tâche avait été exécutée. **Remarque :** **L'exécution d'essai** doit être désactivée lors de la configuration d'une tâche de confidentialité des données avec restauration. Consultez Restauration de la tâche de confidentialité des données pour en savoir plus.
Type de sélection de l'utilisateur	Sélectionnez les utilisateurs ou les groupes à anonymiser.
Sélectionner des utilisateurs/groupes	Sélectionnez un ensemble spécifique d'utilisateurs ou de groupes à anonymiser dans cette tâche. Prend en charge jusqu'à 1 000 utilisateurs. **Remarque :** Ce champ obligatoire s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée nécessite une sélection d'enregistrements utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Important :**
   Toutes les tables doivent avoir une entrée sys_dictionary correcte avant la planification et pendant la tâche.

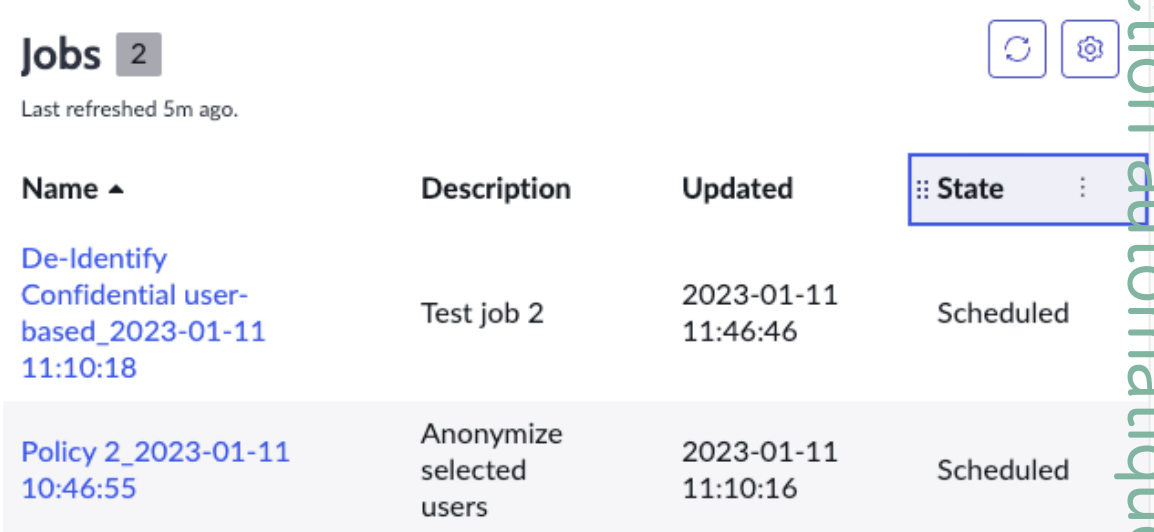
   Sélectionnez **Planifier la tâche** sur le formulaire pour placer l'anonymisation dans la file d'attente de la tâche.

   La tâche s'exécute entre les heures sélectionnées dans les champs **Heure de début** et **Heure de fin** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, la tâche se poursuivra au début de la fenêtre d'heure suivante.

   Une tâche ne peut être exécutée qu'une seule fois, même si **l'option Exécution d'essai** est sélectionnée. Pour exécuter à nouveau une tâche basée sur la même politique, sélectionnez **Planifier une tâche** et remplissez le formulaire en utilisant les mêmes valeurs de champ.

   Avertissement :
   Les tâches d'anonymisation sur les colonnes chiffrées vous permettent de déchiffrer et de chiffrer à nouveau toutes les colonnes chiffrées ciblées par la tâche. Pour éviter cela, sélectionnez **Aucune action** comme technique de politique.

   La tâche est répertoriée dans le volet



Tâches .

Champ	Description
Nom	Nom de la tâche d'anonymisation.
Description	Description de la tâche d'anonymisation.
Mis à jour	Date et heure de la dernière mise à jour de la tâche.
État	État de la tâche de confidentialité des données : ○ **Planifié** : état par défaut des nouvelles tâches. ○ **Terminé** : la tâche a anonymisé avec succès les données sélectionnées. ○ **Annulé** : la tâche a été annulée manuellement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Erreur** : un problème est survenu lors de l'enregistrement de la tâche. Replanifiez la tâche ou créez une nouvelle tâche. Il peut y avoir des problèmes avec la configuration si l'erreur persiste. ○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la tâche d'anonymisation est terminée avec succès. Champ en lecture seule.

6. Sélectionnez une tâche dans le volet **Tâches** pour ouvrir le résumé de la tâche.
Une fois qu'une tâche est planifiée, les boutons **Annuler la tâche** et **Mettre en pause** apparaissent dans le résumé de la tâche.

Champs supplémentaires pour les travaux planifiés

Champ	Description
Estimer le nombre d'enregistrements	Nombre estimé d'enregistrements que cette tâche d'exécution d'essai affecte avant d'être exécutée. Champ en lecture seule
Nombre total d'enregistrements de données traités	Nombre total d'enregistrements de données individuels affectés par cette tâche. Champ en lecture seule.
Nombre total de tables de données traitées	Nombre total de tables de données traitées par cette tâche. Champ en lecture seule.
Temps restant pour la restauration	Durée restante pendant laquelle une tâche d'anonymisation des données terminée peut être restaurée et désanonymiser les données. Champ en lecture seule.
Nombre total d'utilisateurs traités	Nombre total d'enregistrements d'utilisateurs individuels que cette tâche affecte. Champ en lecture seule.
Annuler le travail	Sélectionnez cette option pour annuler la tâche d'anonymisation. Cette option doit être sélectionnée avant l'heure de début de la tâche. Lorsque cette option est sélectionnée, l'état de la tâche est défini sur *Annulé*.
Mettre en pause	Sélectionnez cette option pour mettre en pause la tâche et restaurer l'enregistrement, si la restauration a été sélectionnée. Un message d'avertissement s'affichera après une période d'expiration de trois jours pour les contextes de restauration. Cette option doit être sélectionnée après l'heure de début de la tâche et avant l'heure de fin de la tâche. Lorsque cette option est sélectionnée, l'état de la tâche passe à *Pause*.
Reprendre	Redémarre une tâche en pause. La restauration n'est pas prise en charge pour les travaux repris en cas de pause. Annulez la tâche et créez une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsque cette option est sélectionnée, l'état de la tâche bascule sur `Planifié`.
Exporter	Télécharge un fichier .PDF des détails de la tâche de confidentialité des données.

Activer les tâches parallèles pour l'anonymisation des données

Utilisez des tâches parallèles pour réduire le temps d'exécution de votre tâche d'anonymisation.

Avant de commencer
Rôle requis : admin

Procédure
Par défaut, les tâches d'anonymisation basées sur la classe de données et l'utilisateur s'exécutent à l'aide d'un seul thread. Plusieurs threads peuvent être activés pour les travaux basés sur la classe de données et l'utilisateur. De plus, les tâches fédérées utilisées lors du clonage utilisent des tâches parallèles avec 3 workers par défaut.

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Créer la propriété `com.glide.data_privacy.max_parallel_workers`
3. **Facultatif :** Pour ajuster le nombre d'agents parallèles de tâche fédérés, modifiez la propriété `dp.max_concurrent_clone_item_workers` .
4. Vérifiez que le **type** est un nombre entier.
5. **Important :**
   Il est recommandé de commencer avec un petit nombre de travailleurs par nœud (2 ou 3).

   Saisissez le nombre d'agents parallèles dans le champ **Valeur** jusqu'à 5.

Anonymisation en temps réel

Utilisez la politique d'anonymisation en temps réel (RTA) pour anonymiser les entrées de données en temps réel.

Vue d'ensemble de l'anonymisation en temps réel

Les utilisateurs créent une politique RTA en sélectionnant l'anonymisation en temps réel dans la page Politiques d'anonymisation, puis en sélectionnant le canal de données approprié. Par exemple, vous pouvez utiliser Agent virtuel avec l'anonymisation en temps réel : créez une politique d'anonymisation avec le Agent virtuel canal de **données** sélectionné.

Des colonnes des tables cibles peuvent être sélectionnées pour RTA, après quoi des schémas de données actifs sont utilisés et leurs politiques appliquées à toutes les entrées d'enregistrement valides dans les colonnes ciblées pour RTA. Si une entrée correspond à un modèle de données actif, sa technique d'anonymisation associée sera utilisée pour l'anonymisation.

Conseil :
Si vous devez modifier la technique d'anonymisation, reportez-vous à la section Configurer des Détection de données schémas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échecs d’anonymisation en temps réel

Si une politique RTA échoue, vous pouvez examiner son état avec la Échecs d’anonymisation en temps réel table.

Échecs d’anonymisation en temps réel

Examinez les échecs d’anonymisation en temps réel (RTA).

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Confidentialité des données (classique)**.
2. Examinez les échecs RTA dans la table.

Titre de champ	Description
Colonne de table	Colonne de table dans laquelle l’échec s’est produit.
Cause de la défaillance	Catégorie de la cause des défaillances.
Détails de la raison de la défaillance	Brève description résumant la cause de l’échec.
Configuration de la confidentialité	La configuration de la confidentialité RTA qui a échoué.
Enregistrement	L’enregistrement spécifique qui a échoué.
Nom de la table	Table dans laquelle l’échec s’est produit.
Horodatage	Heure de l’échec.

Activer la confidentialité des données

La confidentialité des données comprend la classification et l’anonymisation ServiceNow Store des données et est installée à partir du .

Avant de commencer
Pour utiliser l’anonymisation des données, Confidentialité des données (classique) doit d’abord être activé avec l’autorisation ServiceNow Coffre-fort . Consultez Activer la confidentialité des données (classique) pour plus d'informations.

Remarque :
L’installation de l’application Data Privacy Store installe automatiquement l’application Data Discovery Store, le module d’extension Data Privacy (Classic) et le module d’extension Data Classification.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous** > **Confidentialité des données**.
2. Utilisez les critères de filtre et la barre de recherche pour trouver l'application.

   Vous pouvez rechercher l'application à l'aide de son nom ou de son ID. Si vous ne trouvez pas l'application que vous recherchez, vous devrez peut-être la demander auprès du ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

3. Sélectionnez une version de la liste et sélectionnez **Installer**.

   La boîte de dialogue Installer qui s'affiche répertorie toutes les dépendances installées avec votre application.

4. Si vous y êtes invité, suivez les liens vers le ServiceNow Store afin d'obtenir des autorisations supplémentaires pour les dépendances.

5. **Facultatif :** Si des données de démonstration sont disponibles et que vous souhaitez les installer, cochez la case **Charger les données de démonstration**.

   (Optional) Les données de démonstration comprennent des exemples d'enregistrements décrivant les fonctionnalités des applications pour les cas d'utilisation fréquents. Chargez les données de démonstration lors de la première installation de l'application sur une instance de développement ou de test.

   Important :
   Les données de démonstration ne sont pas disponibles pour un chargement ultérieur si vous ne les chargez pas lors de l'installation.

6. Sélectionnez **Installer**.

Confidentialité des données pour Agent virtuel

Vous pouvez utiliser la confidentialité des données pour détecter et masquer les données sensibles et les informations personnelles lors d'une conversation avec l'Agent virtuel.

Avant de commencer

Rôle requis : virtual_agent_data_privacy_admin

Pourquoi et quand exécuter cette tâche

Utilisez Confidentialité des données pour détecter et masquer les données sensibles et les PII au cours d'une conversation avec Agent virtuel. La confidentialité des données remplace le gestionnaire de données sensibles déprécié, voir Processus de dépréciation [KB0867184] pour plus d'informations. Le processus de configuration peut varier selon que le gestionnaire de données sensibles a été installé et configuré précédemment.

Remarque :
Si vous avez déjà configuré le gestionnaire de données sensibles, vos paramètres seront migrés vers Confidentialité des données en tant que politique. Consultez Créer des politiques d'anonymisation pour plus d'informations.

Procédure

1. Accédez à la **Tous** > **Interfaces conversationnelles** > **Paramètres**.
2. Sous **Détection de données sensibles**, sélectionnez **Afficher tout**.
   Si le bouton indique **Obtenir la confidentialité des données**, vous devrez installer le module d'extension Confidentialité des données pour continuer. Pour plus d'informations, consultez Activer la confidentialité des données (classique)
3. Réglez le curseur sur **Actif**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Facultatif :** Si Data Privacy n’est pas encore installé, vous serez invité à installer le module d’extension Data Privacy pour continuer, consultez Activer la confidentialité des données (classique) pour plus d’informations.
5. Sélectionnez le flux de conversation approprié :
   a. Demandeur à agent : détectez et masquez les données sensibles saisies par le demandeur dans une Messagerie instantanée d'agent conversation.
   b. Agent au demandeur : détectez et masquez les données sensibles saisies par l’agent dans une Messagerie instantanée d'agent conversation.
   c. Demandeur à Agent virtuel : détecter et masquer les données sensibles saisies par le demandeur au cours d’une Agent virtuel conversation.

   Remarque :
   Vous devez sélectionner au moins un flux de conversation.

6. Sélectionnez **Gérer dans Confidentialité des données**.
   Si vous avez déjà configuré Gestionnaire de données sensibles, vos paramètres seront migrés en tant que politique vers Confidentialité des données
7. Créer une nouvelle politique de confidentialité des données pour Virtual Agent, consultez Créer des politiques d’anonymisation pour plus d’informations sur les politiques de confidentialité des données.

Séparation de domaine et confidentialité des données

La séparation de domaine n’est pas prise en charge pour la confidentialité des données. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Aucun

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique métier pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Information associée

Séparation de domaine pour les fournisseurs de services

Types de champs pris en charge pour l’anonymisation

Vérifiez quels types de champs sont pris en charge lors de l’anonymisation des données.

Remarque :
Tous les types de champs qui ont été classés ne sont pas disponibles pour l’anonymisation.

Certains types de champs à risque élevé sont désactivés par défaut, comme indiqué dans la table. Pour plus d’informations sur les champs, voir Types de champs .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de champs pris en charge pour l'anonymisation

Type de champ	Disponible par défaut
audio	Non
condition	Non
condition_string	Non
currency	Oui
décimal	Oui
due_date	Oui
flottant	Oui
glide_date	Oui
glide_date_time	Oui
glide_duration	Non
glide_time	Oui
HTML	Non
icône	Non
entier	Oui
ip_addr	Non
ip_address	Non
journal	Oui
journal_input	Oui
journal_list	Oui
longint	Oui
name_values	Non
percent_complete	Non
phone_number_e164	Oui
prix	Oui
chaîne	Oui
string_full_utf8	Oui
translated_html	Non
translated_text	Non
URL	Non
user_image	Non
vidéo	Non
wiki_text	Non

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles de confidentialité des données

La confidentialité des données ajoute ces rôles.

Administrateur de la confidentialité des données

Les rôles d'administrateur de confidentialité des données sont un rôle administrateur utilisé pour créer des techniques et des politiques de confidentialité des données.

Administrateur de la confidentialité des données [data_privacy_admin]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus ciblés sont disponibles.

Pour affecter le rôle « Administrateur de la confidentialité des données », élevez l'utilisateur au rôle d'administrateur de sécurité afin d'ajouter le rôle.

Auditeur de confidentialité des données

Auditeur de confidentialité des données est un rôle en lecture seule qui permet d'afficher les enregistrements de confidentialité des données.

Auditeur de confidentialité des données [data_privacy_auditor]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Non

Considérations

Aucun

Confidentialité des données Cloner le processeur

Les utilisateurs disposant du rôle de processeur clone de confidentialité des données peuvent créer et exécuter des tâches de confidentialité des données de classe de données.

Processeur clone confidentialité des données [data_privacy_clone_processor]

Contient des rôles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Processeur de confidentialité des données

Les utilisateurs ayant le rôle de processeur de confidentialité des données créent et exécutent des tâches de confidentialité des données sur la table de l'utilisateur [sys_user].

Sous-traitant de la confidentialité des données [data_privacy_processor]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Confidentialité des données (classique)

Confidentialité des données (classique) est une application héritée qui fournit une classification des données, des techniques et des tâches pour anonymiser les Informations personnellement identifiables (IPI).

Confidentialité des données classique

Remarque :
Cette section est destinée à la confidentialité des données (classique). Reportez-vous Confidentialité des données à la dernière version de stockage à jour.

Activer la confidentialité des données (classique)

Vous pouvez activer le module d'extension de confidentialité des données (com.glide.data_privacy) si Platform Security vous disposez du rôle administrateur. L'application inclut des données de démonstration et installe les applications et modules d'extension connexes ServiceNow® Store , le cas échéant.

Avant de commencer

Important :
Cette section est destinée à la confidentialité des données (classique). Reportez-vous Confidentialité des données à la dernière version de stockage à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La confidentialité des données nécessite un abonnement distinct du reste du ServiceNow AI Platform®.

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si un module d'extension acheté n'est pas activé automatiquement, vous pouvez l'activer manuellement à partir de la liste Toutes les applications de votre instance.

Remarque :
Avant d'acheter un abonnement, vous pouvez évaluer Data Privacy (Classic) et Data Discovery avec une période d'essai de 30 jours. Après l'expiration de votre essai, vous ne pourrez plus détecter de données ou exécuter des tâches d'anonymisation sans licence.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec Confidentialité des données :

- Modules d'extension
- Rôles
- Tables

Pour plus d'informations, consultez Installé avec Confidentialité des données (classique).

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Data Privacy (com.glide.data_privacy) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application.

Installé avec Confidentialité des données (classique)

Découvrez les composants installés avec le module d'extension Confidentialité des données (com.glide.data_privacy).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées

Table	Description
Tâche fédérée Confidentialité des données [dp_federated_job]	Tâches fédérées pour la confidentialité des données
Tâche de Confidentialité des données [dp_job]	Tâches de confidentialité des données
Tâche de Confidentialité des données [dp_job_summary]	Résumés des tâches de confidentialité des données
Technique de Confidentialité des données [dp_technique]	Techniques de confidentialité des données
Lien de référence primaire [dp_primary_reference]	Liens de référence primaires
Technique de champ classé pour la confidentialité [dp_field_technique]	Techniques de champ classé Confidentialité des données
Configuration de la confidentialité [dp_configuration]	Configurations de confidentialité des données
Configuration de la technique de confidentialité [dp_technique_with_params]	Techniques de confidentialité des données
Paramètre de la technique de confidentialité [dp_technique_with_parameter]	Techniques Confidentialité des données avec paramètres
Valeur de paramètre de la technique de confidentialité [dp_technique_with_parameter_value]	Valeurs des paramètres utilisées dans les techniques de confidentialité des données avec paramètres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de confidentialité des données (classique)

Découvrez comment créer des techniques et des politiques de confidentialité des données, et comment créer et exécuter des tâches de confidentialité des données.

Important :
Cette section est destinée à la confidentialité des données (classique). Reportez-vous Confidentialité des données à la dernière version de stockage à jour.

Techniques de confidentialité des données

Les techniques de confidentialité des données sont des options que vous sélectionnez pour déterminer comment vos données sont anonymisées. Vous devez créer une technique de confidentialité des données à référencer dans la tâche de confidentialité des données. Voir Créer une configuration de la technique de confidentialité des données pour associer une technique de confidentialité à une **configuration de technique de confidentialité** associée.

Politique de confidentialité des données

Configurez une politique de confidentialité des données pour spécifier les techniques de confidentialité des données utilisées lors de l'anonymisation de vos données. Consultez Créer une politique de confidentialité des données pour en savoir plus.

Tâches de confidentialité des données

Les tâches de confidentialité des données utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces emplois, reportez-vous à Configurer une tâche de confidentialité des données.

Créer une configuration de la technique de confidentialité des données

Créez une configuration de technique de confidentialité des données pour personnaliser la façon dont la confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et administrateur

Procédure

1. Accéder au rôle **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Configuration de la technique de confidentialité**.
3. Cliquez sur **Nouveau**.
4. Dans le champ **Nom** , saisissez un nom pour la configuration de votre technique de confidentialité.
5. Dans le champ **Technique de confidentialité** , sélectionnez une technique de confidentialité.

Techniques de confidentialité des données

Technique	Description
Aucune action	Cette technique est un espace réservé. Il ne modifie pas les champs lorsqu'ils sont sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Technique	Description
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de façon aléatoire. Les données chaîne et numéro peuvent utiliser cette technique.
Remplacement sélectif	Cette technique remplace sélectivement les données de chaîne. Tous les caractères entre les index de début et de fin de l'entrée sont remplacés par le caractère que vous choisissez. Vous pouvez spécifier des caractères à exclure du masquage : ○ start_index : la technique masque les données commençant par le caractère spécifié. S'il est laissé vide, le masquage commence par le premier caractère. ○ end_index : la technique masque les données du début de la chaîne jusqu'au caractère spécifié. Si ce champ est laissé vide, le masquage se termine au dernier caractère. ○ exclude_char : définissez un caractère à exclure du masquage. ○ replacement_char : Définissez un caractère utilisé pour le masquage. Si aucun n'est fourni, les astérisque (*) sont utilisés par défaut.
Remplacement statique	Cette technique échange les valeurs avec des valeurs statiques. Les données chaîne, numéro et date peuvent utiliser cette technique : ○ date_time_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss. ○ date_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj. ○ number_value : remplacez les valeurs de nombres par ce nombre. ○ string_value : remplacez les valeurs de chaîne par ce texte.
Supprimer	Cette technique supprime les valeurs et les remplace par des valeurs vides (null).

Remarque :
Valeur précédemment prise en charge **Le remplacement** est déconseillé et renommé **Remplacer-Déconseillé** et ne doit pas être utilisé.

6. Cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer** dans le menu contextuel.
   Une fois l'enregistrement enregistré, la liste **des valeurs paramétrées de confidentialité** s'affiche.
7. Utilisez les enregistrements de la liste **Valeurs paramétrées de confidentialité** pour personnaliser la configuration de votre technique de confidentialité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les valeurs paramétrées disponibles dépendent de la technique de confidentialité que vous avez sélectionnée. Il n'existe aucune valeur paramétrée pour les techniques **Aucune action** et **Supprimer** .

Valeurs paramétrées de confidentialité pour le remplacement sélectif

Valeur du paramètre de la technique de confidentialité	Description	Valeur par défaut
char_to_replace	Caractère à utiliser lors du remplacement de valeurs à l'aide d'un remplacement sélectif.	*
end_index	La technique masque les données du début de la chaîne jusqu'au caractère spécifié. S'il est laissé vide, le masquage se termine au dernier caractère.	(Vide)
exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plusieurs caractères sont saisis, le premier caractère est utilisé.	(Vide)
start_index	La technique masque les données commençant par le caractère spécifié.	1

Valeurs paramétrées de confidentialité pour Remplacer

Valeur du paramètre de la technique de confidentialité	Description	Valeur par défaut
date_time_value	Remplacez les valeurs de date et d'heure par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss.	1988-11-11 10:10:10
date_value	Remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj.	1988-11-11
number_value	Remplacez les valeurs de nombres par ce nombre.	1234567
preserve_data_length	Définissez la valeur **sur vrai** pour préserver la longueur des données. Les données dé-identifiées auront la même longueur que les données d'origine.	vrai
string_value	Remplacez les valeurs de chaîne par ce texte.	TEXT123
use_random_generated_value	Définissez la valeur **sur vrai** pour remplacer les données par des valeurs générées de façon aléatoire. Seules les données chaîne et numéro peuvent être remplacées par des valeurs	Faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur du paramètre de la technique de confidentialité	Description	Valeur par défaut
	aléatoires. Cette option remplace les valeurs statiques.	

8. Cliquez sur **Enregistrer**.

Créer une politique de confidentialité des données

Configurez une politique de confidentialité des données pour spécifier les techniques de confidentialité des données utilisées lors de l'anonymisation de vos données.

Avant de commencer

La configuration de confidentialité des données définit les tables, les sys_user et autres, et les colonnes à désidentifier, en fonction du cas d'utilisation, et spécifie les types paramétrés des techniques à utiliser lors de la désidentification des données.

Remarque :
Pour terminer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez Créer une configuration de la technique de confidentialité des données pour plus d'informations.

Rôle requis : data_privacy_admin et administrateur

Procédure

1. Accéder au rôle **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données (classique)** > **Configuration de la politique de confidentialité**.
3. Sélectionnez **Nouveau**.
4. Dans le champ **Nom** , saisissez un nom pour la configuration de votre politique de confidentialité.
5. Dans le champ **Classe de données** , sélectionnez la classe de données à utiliser avec cette stratégie.
   Les politiques de confidentialité des données ne peuvent s'appliquer qu'aux données classifiées. Pour plus d'informations sur la classification des données, consultez Classification des données.
   Après avoir sélectionné une classe de données, les listes **Techniques de champ classé pour la confidentialité** et **Liens de référence primaires** pour la confidentialité s'affichent sur le formulaire.
6. **Facultatif :** Sélectionnez **Appliquer à toutes les données de la classe** pour appliquer l'anonymisation à toutes les données de la classe de données choisie.
   Si vous ne sélectionnez pas ce champ, vos utilisateurs de votre processeur de confidentialité des données peuvent choisir les utilisateurs à anonymiser lors de la création de tâches de confidentialité des données. Si vous sélectionnez ce champ, cette option n'est pas disponible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Appliquer lors du clonage** : Cette option devient disponible. Quand cette option est sélectionnée, la configuration de la confidentialité s'exécute pendant le clonage de la confidentialité des données.
- **Ordre d'application** : une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application supérieur peut commencer avant une autre tâche d'ordre inférieur.

> **Important :**
> Évitez de créer plusieurs politiques de confidentialité des données avec la même commande d'application, car l'ordre de traitement résultant pour celles qui ont la même commande sera incohérent.

7. **Facultatif :** Sélectionnez **Prend en charge la restauration** pour activer la possibilité de désanonymiser les données d'une tâche de confidentialité des données.
   Consultez Restaurer une tâche de confidentialité des données pour plus d'informations.
   Après avoir sélectionné **Prend en charge la restauration** lors de la création d'une tâche de confidentialité des données, l'option de restauration de la tâche devient disponible.
8. Sélectionnez l'onglet **Techniques de champ classé** pour la confidentialité pour afficher la liste **des techniques de champ classées pour la confidentialité** .
9. Sélectionnez une entrée dans le champ **Table** pour ouvrir le champ Configuration de la **technique de confidentialité** pour chaque entrée de liste.
   La liste **Techniques de champ classé pour la confidentialité** affiche toutes les données à anonymiser dans la classe de données que vous avez sélectionnée. Pour chacune de ces entrées, vous devez sélectionner une technique de confidentialité à appliquer.
10. Sélectionnez une **configuration de technique de confidentialité** à appliquer.

> **Important :**
> Si vous n'anonymisez pas une entrée, sélectionnez la technique **Ne rien faire** plutôt que de laisser l'entrée vide. Les politiques avec des valeurs vides dans le champ Configuration de la **technique de confidentialité** ne peuvent pas s'exécuter lorsqu'elles sont utilisées dans les tâches de confidentialité des données.

11. Sélectionnez **Soumettre** ou **Enregistrer** pour enregistrer l'enregistrement.

Que faire ensuite

Configurer une tâche de confidentialité des données.

Configurer une tâche de confidentialité des données

Configurez une tâche de confidentialité des données sur votre instance de production pour utiliser des données rendues anonymes sur votre instance de non-production pour les tâches d'utilisateur et de classe de données.

Avant de commencer

La tâche de confidentialité des données prend en charge deux cas d'utilisation de désidentification :

- Données sensibles d'sys_users spécifiques
- Données sensibles d'une classe de données particulière.

Rôle requis : data_privacy_processor et admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Élevez-vous au rôle **data_privacy_processor** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Tâche de Confidentialité des données**.
3. Dans la liste Tâches de confidentialité des données, cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire.

Champs des tâches de confidentialité des données

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Configuration de la confidentialité	La configuration de la politique de confidentialité à utiliser pour cette tâche. Pour en savoir plus sur les configurations de la politique de confidentialité, reportez-vous à la section Créer une politique de confidentialité des données.
Fréquence	○ **Exécuter une fois** : la tâche s'exécutera une fois dans la fenêtre de temps spécifiée. ○ **Hebdomadaire** : la tâche s'exécutera chaque jour du champ **Jour de la semaine** dans la fenêtre horaire spécifiée. ○ **Mensuel** : la tâche s'exécutera chaque jour du mois tel qu'entré dans **le champ Jour du mois** dans la fenêtre de temps spécifiée.
Utilisateurs	Sélectionnez les utilisateurs ou le groupe d'utilisateurs à anonymiser dans cette tâche. Jusqu'à 1000 utilisateurs d'un groupe peuvent être traités. **Remarque :** Ce champ s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée nécessite une sélection d'enregistrements utilisateur.
Essai	Exécutez la tâche comme un test. Aucun enregistrement n'est affecté lors de l'exécution de cette tâche. Les résultats sont affichés dans le champ **Résumé** comme si la tâche avait été exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : **L'exécution d'essai** doit être désactivée lors de la configuration d'une tâche de confidentialité des données avec restauration. Consultez Restaurer une tâche de confidentialité des données pour en savoir plus.
État	État de la tâche de confidentialité des données : ○ **Terminé** : tâche terminée avec succès. ○ **Prêt à planifier** : état par défaut des nouvelles tâches. ○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la tâche d'anonymisation est terminée avec succès. ○ **Terminé avec des erreurs** : la tâche est terminée, mais comporte des erreurs. Consultez Journaux de tâche de Confidentialité des données pour plus d'informations. ○ **Erreur** : la tâche ne s'est pas terminée et présente une erreur. Pour plus d'informations, consultez Journaux de tâche de Confidentialité des données Champ en lecture seule.
Estimer le nombre d'enregistrements	Nombre estimé d'enregistrements affectés par cette tâche. Champ en lecture seule.
Résumé	Champ en lecture seule qui affiche les résultats de la tâche lorsque vous l'exécutez.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ. Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.
Fin de la fenêtre de temps	La fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, elle sera mise en pause et reprendra au début de la fenêtre d'heure suivante. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez avec le bouton droit dans l'en-tête du formulaire et sélectionnez **Enregistrer** dans le menu contextuel.
   Après avoir enregistré l'enregistrement, les boutons **Planifier** la **tâche** et Supprimer la tâche s'affichent.
6. Cliquez sur **Planifier la tâche** pour exécuter votre tâche.
   La tâche s'exécute entre les heures sélectionnées dans les champs Début de la **fenêtre** horaire et Fin de la **fenêtre horaire** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, la tâche se poursuivra au début de la fenêtre d'heure suivante.

   Remarque :
   Une tâche ne peut être exécutée qu'une seule fois, même si **l'option Exécution d'essai** est sélectionnée. Pour exécuter à nouveau le même travail, créez une tâche de confidentialité des données à l'aide des mêmes valeurs de champ.

7. **Facultatif :** Choisissez l'une des fonctions suivantes :
   - **Annuler la tâche** : annule la tâche de confidentialité des données.
   - **Pause** : met en pause la tâche et l'enregistrement de restauration, si la restauration a été sélectionnée. Un message d'avertissement s'affichera après une période d'expiration de trois jours pour les contextes de restauration. Consultez Restaurer une tâche de confidentialité des données pour en savoir plus.
   - **CV** : redémarre une tâche en pause. La restauration n'est pas prise en charge pour les travaux repris en cas de pause. Annulez la tâche et créez une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré.

Restauration de la tâche de confidentialité des données

Les changements apportés à la base de données sont capturés pour des actions telles que des tâches et des scripts afin que les changements puissent être restaurés. Restaurez une tâche de confidentialité des données lorsqu'une erreur humaine anonymise par inadvertance des informations utilisateur incorrectes. La restauration désanonymise les données de la tâche de confidentialité des données.

Vue d'ensemble

- La restauration est limitée à quelques jours, selon la durée d'expiration configurée du RollbackContext du nouveau RollbackType *`REDACT`*. Après l'expiration du RollbackContext associé à une tâche de confidentialité des données, la fonction de restauration n'est plus disponible pour cette tâche.
  - Un contexte de restauration issu de la désanonymisation est enregistré pendant trois jours par défaut.
  - Le délai d'expiration par défaut peut être défini sur une valeur supérieure à une par l'administrateur de la confidentialité des données dans le **RollbackContext** du nouveau **RollbackType** *`REDACT`*. Définissez la valeur dans la propriété *`glide.rollback.expiration_days_redact`*système Glide . Consultez Roll back and delete recovery .

    Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

    pour plus d'informations.
- La restauration est disponible pour les tâches de confidentialité des données qui sont à l'état Terminé, Annulé ou Erreur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour chaque tâche de désanonymisation réussie sys_user configurée avec une politique de confidentialité des données avec la prise en charge de la restauration activée, un contexte de restauration est créé. Il peut y avoir au maximum un contexte de restauration par tâche de confidentialité des données.

Restaurer une tâche de confidentialité des données

Restaurez une tâche de confidentialité des données sur votre instance de non-production qui utilise des données anonymisées de votre instance de production à un état avant la désidentification d'une classe de données ou d'une tâche utilisateur.

Avant de commencer

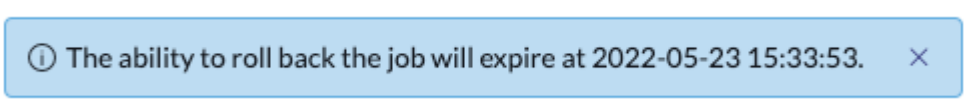
Rôle requis : data_privacy_admin ou data_privacy_processor et administrateur

Procédure

1. Accéder au **rôle data_privacy_processor** ou **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Tous** > **Sécurité de système** > **Confidentialité des données** > **Tâche de Confidentialité des données**.

   Remarque :
   Au préalable, une configuration de politique de confidentialité des données prenant en charge la restauration doit être créée. Créer une politique de confidentialité des données.

3. Créez une tâche de confidentialité des données et sélectionnez une configuration de confidentialité qui prend en charge la restauration.
   Consultez Configurer une tâche de confidentialité des données.
4. Planifiez la tâche pour l'anonymisation des données.
   - Une fois la tâche exécutée, les données sont anonymisées pour la configuration sélectionnée.
   - Un message s'affiche dans la tâche pour informer du délai d'expiration. Pendant la période d'expiration, vous avez la possibilité de restaurer la tâche.

5. Élevez-vous au rôle **data_privacy_processor** .
6. Ouvrez la tâche de confidentialité des données à restaurer.
7. Sélectionnez **Restaurer** pour désanonymiser les données.

Clone de confidentialité des données

Au fur et à mesure que les données client sont clonées d'une instance source vers une instance cible, généralement de la production à la non-production, les données sensibles sont dépersonnalisées sur l'instance cible.

Important :
Cette section est destinée à la confidentialité des données (classique). Reportez-vous Confidentialité des données à la dernière version de stockage à jour.

Un administrateur de la confidentialité des données configure les politiques post-clone. Une fois le script post-clone terminé sur l'instance cible, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine. Les administrateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de confidentialité des données peuvent configurer des politiques de désidentification à appliquer sur l'instance cible lors du clonage afin de s'assurer que l'instance cible ne comportera pas de données sensibles d'origine. Un ordre est spécifié pour la politique par rapport aux autres politiques à exécuter.

Remarque :
Le clonage de la confidentialité des données n'est pas disponible sur les instances auto-hébergées.

Le clone de confidentialité des données comporte les attributs supplémentaires suivants :

- Le module d'extension Confidentialité des données crée le script de post-clonage à exécuter sur l'instance cible.
- Les tâches de confidentialité des données créées pour la configuration PostClone peuvent s'exécuter en parallèle si elles n'impliquent pas les mêmes tables.
- Une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application supérieur peut commencer avant une autre tâche d'ordre inférieur, si la tâche avec l'ordre supérieur n'implique aucune table liée à une autre tâche d'ordre inférieur.
- Avec le module d'extension Confidentialité des données, les tables de confidentialité des données se trouvent par défaut dans l'ensemble de tables Conservateurs de données de clone.
- Toute tentative d'ajout d'une table de confidentialité des données (dp_[table]) à Cloner les tables d'exclusion recevra un avertissement, cette table ne doit pas être exclue.

Configurer la demande de clone de confidentialité des données

L'intégration de clone de confidentialité des données est configurée à l'aide d'un script PostClone pour créer et exécuter des tâches de confidentialité des données pour les politiques configurées sur la cible. Une fois le script exécuté, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine.

Avant de commencer
Rôle requis : data_privacy_clone_processor, data_privacy_admin et admin

Procédure

1. Activez le module d'extension de confidentialité des données (sn_dp_store_app) sur l'instance source.
   Le module d'extension ne peut être installé que par Service client et assistance.
   Le script PostClone de confidentialité des données est installé.
2. Accéder au rôle **data_privacy_admin** .
   Pour plus de détails sur l'élévation de rôle, consultez Élever à un rôle privilégié.
3. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Configuration de la politique de confidentialité**.
4. Créez une configuration de politique de confidentialité.
   Sélectionnez **Appliquer à tous dans la classe de données** et **Appliquer lors du clonage**.
   Consultez Créer une politique de confidentialité des données pour plus d'informations.
5. Sauvegardez les configurations de confidentialité des données.
6. En tant qu'administrateur de la confidentialité des données, soumettez une demande de clone.

Résultats
Le script PostClone de confidentialité des données s'exécute sur l'instance cible et le script PostClone crée un enregistrement de tâche fédérée de confidentialité des données sur l'instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour chaque politique post-clone, dans l'ordre de l'application, sur l'instance cible.La source de sauvegarde est clonée sur l'instance cible. Le script PostClone de confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l'instance cible.

Le processeur clone de confidentialité des données élevée peut se connecter à l'instance cible et surveiller l'état de la tâche fédérée post-clonage sur dp_federated_job.list et dp_job.list.

Journaux de tâche de Confidentialité des données

Examinez les erreurs des tâches de confidentialité des données.

Avant de commencer

Important :
Cette section est destinée à la confidentialité des données (classique). Reportez-vous Confidentialité des données à la dernière version de stockage à jour.

Rôle requis : data_privacy_admin, data_privacy_clone_processor, data_privacy_processor data_privacy_auditor

Pourquoi et quand exécuter cette tâche

Utilisez les **journaux des tâches de confidentialité des données** pour examiner les tâches de découverte, de classification et d'anonymisation qui ont échoué.

Procédure

1. Accédez à la **Sécurité de système** > **Confidentialité des données (classique)** > **Journaux de tâche de Confidentialité des données**.
2. Passer en revue la table

Table des journaux des tâches de confidentialité des données

Étiquette	Description
Créées	Qui ou quoi a créé l'entrée de journal
Niveau	La gravité de l'erreur
Message	Description de la cause de l'erreur
Source	Module d'extension source de l'erreur
Type	Type d'erreur qui s'est produite
Code	Code d'erreur qui s'est produit
Nom de table de la tâche	Table dans laquelle se trouve la tâche
ID de tâche	ID de la tâche
Nom de la table cible	Table sur laquelle la tâche a été exécutée
Colonne de table cible	Colonne sur laquelle la tâche a été exécutée
Enregistrement de la table cible	Enregistrer la tâche exécutée le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détection de données

Utilisez cette fonction Détection de données pour identifier les données sensibles au sein d'une instance, telles que les informations de carte de crédit, les e-mails ou les numéros de sécurité sociale.

Explorer la découverte de données



En savoir plus sur la découverte de données.

Configurer la découverte des données



Obtenez de l'aide pour configurer la découverte de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles dans la découverte des données



En savoir plus sur les rôles dans la découverte des données.

Résultats de découverte de données



Passez en revue les résultats de la découverte de données.

Traduction automatique

Exploration Détection de données (classique)

Utilisez cette fonction Détection de données pour identifier les données sensibles au sein d'une instance, telles que les informations de carte de crédit, les e-mails ou les numéros de sécurité sociale.

Détection de données Exécute un ensemble de tâches défini par l'utilisateur sur un ensemble de tables. Les tâches recherchent et signalent des informations sensibles à examiner sur le tableau de Détection de données bord. Une tâche planifiée utilise automatiquement tous les schémas de données actifs et les tables cibles lorsqu'elle s'exécute.

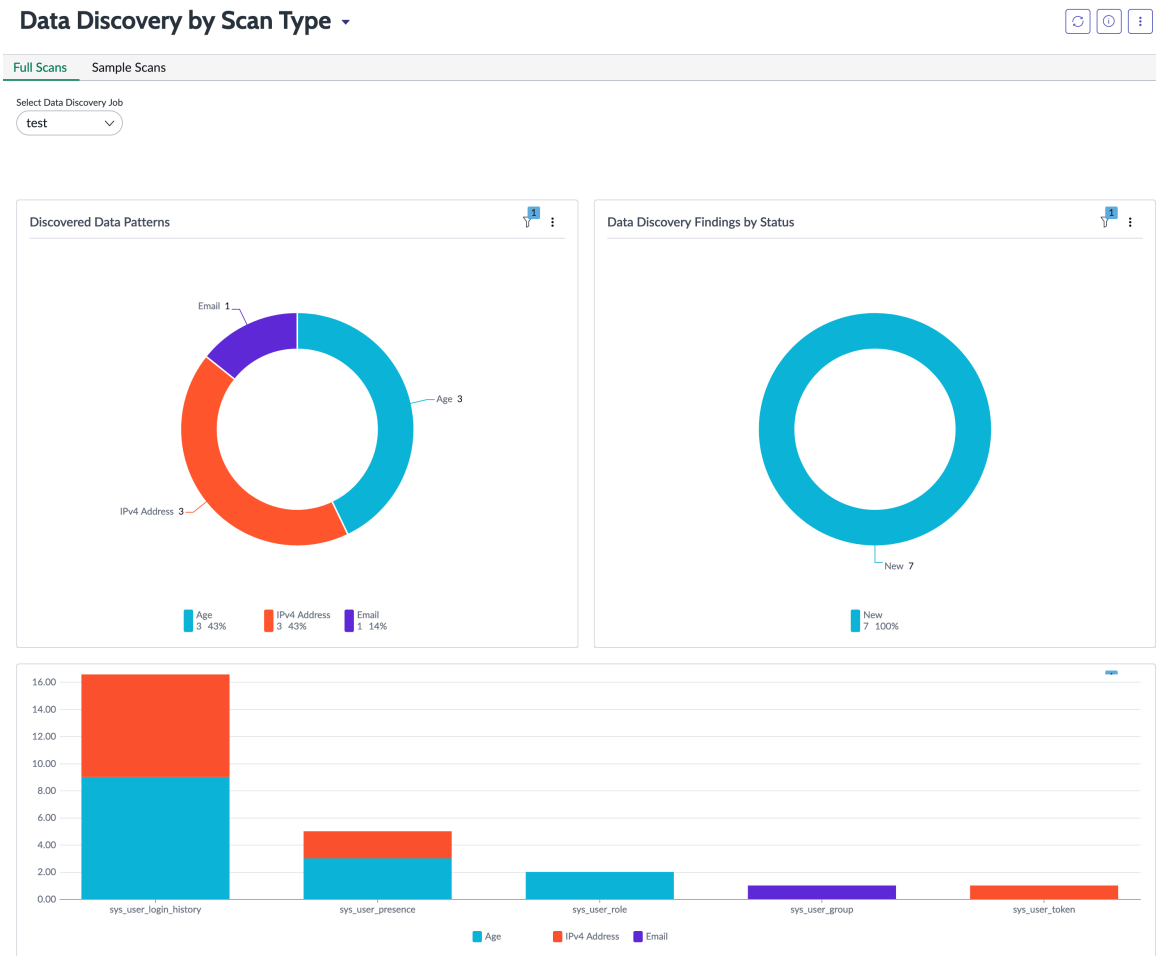
Détection de données comprend également des rôles préalloués avec différents niveaux d'accès aux données.

Accéder au tableau de bord Détection de données

Accédez à la **Tous** > **Sécurité de système** > **Découverte de données (classique)** > **Tableau de bord** pour afficher le Détection de données tableau de bord et examiner vos résultats de tâches actuels.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de Détection de données



Schémas de données détectés

Conseil :
Sélectionnez un enregistrement pour afficher plus d'informations et prendre des mesures supplémentaires en fonction des résultats. Voir Détection de données Résultats des tâches pour plus.

Le graphique Schémas de données détectés affiche le nombre et le pourcentage de schémas de données actuellement détectés. Sélectionnez une section pour prendre des mesures supplémentaires.

Résultats de découverte de données par état

Le graphique Résultats de la découverte des données examine le nombre et le pourcentage de schémas de données actuellement détectés par leur état.

Tables détectées

Les tables détectées mettent en évidence les tables dans lesquelles se trouvent les données actuellement détectées et leur modèle de données.

Colonnes avec données détectées

La section Colonnes avec données détectées examine les données actuellement détectées par leur colonne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer Détection de données

L’application s’installe ainsi que les Détection de données applications et modules d’extension connexes ServiceNow® Store , le cas échéant.

Avant de commencer

La découverte de données nécessite un abonnement distinct du reste du ServiceNow AI Platform.

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si un module d'extension acheté n'est pas activé automatiquement, vous pouvez l'activer manuellement à partir de la liste Toutes les applications de votre instance.

Remarque :

Avant d'acheter un abonnement, vous pouvez évaluer la fonctionnalité sur une instance de non-production sans frais en la demandant auprès du Now Support Catalogue de services.

L’installation de l’application de stockage de découverte de données installera automatiquement le module d’extension API de découverte de données

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec la découverte des données :

- Rôles
- Tables

Pour en savoir plus sur les rôles et les tables installés, consultez Détection de données rôles et Schémas de données par défaut.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d’extension Découverte de données (sn_data_discovery) à l’aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d’informations sur les composants installés avec un module d’extension, voir Rechercher les composants installés avec une application .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Classer les données dans la Détection de données page Résultats

Classez les données sensibles trouvées par toutes les tâches réussies via Détection de données des résultats.

Avant de commencer

Rôles requis : data_discovery_admin

Une tâche doit terminer une exécution réussie avant qu'une donnée de résultat puisse sembler classifiée.

Pourquoi et quand exécuter cette tâche

La Détection de données page Résultats affiche toutes les entrées de données qui ont été trouvées par une tâche. La page Résultats vous permet d'examiner les entrées et de les associer à une classification.

Procédure

1. Accédez à la **Sécurité de système** > **Découverte de données (classique)** > **Résultats de découverte de données**.
2. Sélectionnez l'entrée que vous souhaitez classer.
3. Dans la Détection de données liste Résultats, sélectionnez **Classifier**.
4. Sélectionnez les classes de données que vous souhaitez associer aux entrées de table.
5. Sélectionnez **Classifier**.

Détection de données Emplois

Détection de données Examine vos informations ciblées à l'aide de schémas de données définis par l'utilisateur et de tables cibles.

Détection de données fonctionne en planifiant d'abord une tâche dans la section **Tâche de découverte de données** . Lorsqu'une tâche planifiée s'exécute, tous les schémas de données actifs sont recherchés sur les tables cibles actuelles. Pour plus d'informations sur la création et la configuration d'une Détection de données tâche, reportez-vous à la section Configurer une Détection de données tâche.

Remarque :
Les travaux d'analyse d'échantillons analysent jusqu'à 10 000 enregistrements par table et par modèle.

Avertissement :
Si une tâche est exécutée deux fois en peu de temps, le nombre de lignes analysées peut renvoyer 0 pour la deuxième exécution.

Détection de données Schémas de données

La section **Schémas de données** affiche tous les schémas de données actuels, actifs et inactifs. Un modèle de données est une expression régulière utilisée pour mettre en correspondance des données sensibles. Pour plus d'informations sur l'accès aux schémas de données et leur configuration, reportez-vous à la section Configurer des Détection de données schémas. La section **Schémas de données actifs** ne montre que les schémas actifs. Les schémas inactifs n'apparaissent pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables cibles

La section **Tables cibles** répertorie toutes les tables qui peuvent être traitées pour une tâche. Pour accéder aux tables cibles, sélectionnez **Tables cibles**.

Les tables suivantes ne sont pas prises en charge :

- sr
- sysx
- v
- SH$
- syslog
- UA
- UsageAnalytics
- Ecc
- cloner
- JRobin
- papa
- sla_repair_log
- analyse
- Gcf
- fm_log
- journal
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique
- data_classification
- m2m_dictionary_dataclass

Configuration granulaire

L'outil Configuration granulaire active des contrôles plus spécifiques et affinés pour détecter des données sensibles dans une table. Cependant, il existe des différences essentielles dans son fonctionnement par rapport à un travail de découverte de données traditionnel. Une configuration granulaire analyse uniquement les colonnes spécifiées d'une table pour la découverte, en rapportant ses conclusions par enregistrement. Les actions des résultats

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

issus de l'analyse des configurations granulaires, appelées résultats granulaires, sont spécifiées par enregistrement et nécessitent l'anonymisation du rôle data_privacy_admin.

Configurer une Détection de données tâche

Configurez une Détection de données tâche et passez en revue l'état des tâches en cours. Une Détection de données tâche définit quand un modèle est exécuté sur une table cible.

Avant de commencer

Rôle requis : data_discovery_admin

Procédure

1. Accédez à la **Sécurité de système** > **Découverte de données (classique)** > **Tâche de découverte de données**.
2. Dans la Détection de données liste Tâches, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de Détection de données tâche.

Détection de données Champs des tâches

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Type d'analyse	Nombre d'entrées à analyser. Les états possibles sont les suivants : ○ **Exemple** : Scanne 10 000 entrées. ○ **Incrémentiel** : analyse les modèles de données sensibles dans les enregistrements nouveaux ou modifiés. Ce type d'analyse est récurrent. ○ **Complet** : analyse toutes les entrées.
Politique	La politique de découverte des données à utiliser dans cette tâche. Consultez Politiques Détection de données pour plus d'informations.
Analyser les pièces jointes	Analyse les pièces jointes à la recherche de tout schéma de données sensible. Les images incorporées sous des fichiers .pdf ou .doc ne sont pas analysées pour détecter des données sensibles. ⚠ **Avertissement :** Cette fonctionnalité nécessite l'envoi de vos données à un environnement ServiceNow contrôlé. Avant d'activer, veuillez confirmer que vous avez accepté les termes et conditions supplémentaires requis pour utiliser cette fonctionnalité.
Contexte	Détails de la tâche sur les schémas analysés, les entrées des tables cibles touchées et le temps écoulé.
État	État de la Détection de données tâche. Les états possibles sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Prêt à planifier** : état par défaut des nouvelles tâches. ○ **Planifié** : l'exécution de la tâche est planifiée. ○ **En cours** : la tâche est en cours d'exécution. ○ **Terminé** : la tâche s'est terminée avec succès. ○ **Erreur** : la tâche a cessé de s'exécuter en raison d'une erreur. ○ **Annulé** : la tâche a été annulée. ○ **En pause** : la tâche est en pause.
Résumé	Affiche les résultats de la tâche une fois que vous l'avez exécutée.
Date de début	Définit la date de début de la tâche.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ. L'heure saisie dans le champ **de début de la fenêtre de temps** doit être antérieure à l'heure saisie dans le champ de fin de la **fenêtre de temps** . **Remarque :** Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.
Fin de la fenêtre de temps	La fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute jusqu'à l'heure saisie dans ce champ. Si la tâche n'est pas terminée cette fois-ci, la tâche est interrompue et reprend au début de la fenêtre de temps suivante. L'heure saisie dans le champ **de fin de la fenêtre de temps** doit être postérieure à l'heure saisie dans le champ de début de la **fenêtre de temps** . **Remarque :** Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.

4. Sélectionnez **Soumettre**.
   Les boutons **Planifier la tâche** et **Mettre à jour** s'affichent.
5. Sélectionnez **Planifier une tâche** pour exécuter votre tâche.
   La tâche s'exécute entre les heures sélectionnées dans les champs Début de la **fenêtre** horaire et Fin de la **fenêtre horaire** . Si la tâche n'est pas terminée pendant la fenêtre de début et de fin, la tâche se poursuivra au début de la fenêtre de temps suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. **Facultatif :** Choisissez l'une des fonctions suivantes :
   - **Annuler la tâche** : annule la tâche.
   - **Pause** : met la tâche en pause.
   - **CV** : redémarre une tâche en pause.

Analyse des pièces jointes dans les Détection de données tâches

L'analyse des pièces jointes dans Détection de données vous permet de numériser, de détecter et de générer des rapports sur les données sensibles dans les pièces jointes.

Les données sensibles telles que les numéros de sécurité sociale (SSN), les numéros de carte de crédit et d'autres informations personnelles identifiables (PII) sont souvent contenues dans des pièces jointes. Détection de données analyse des pièces jointes vous permet de détecter et de rapporter des données sensibles dans certaines pièces jointes. La fonction d'analyse des pièces jointes n'est disponible que pour les analyses planifiées.

⚠ Avertissement :
Cette fonctionnalité nécessite l'envoi de vos données à un environnement ServiceNow contrôlé. Contactez votre compte et les équipes d'assistance pour activer la fonctionnalité d'analyse des pièces jointes

Limitations

- Les images et pièces jointes incorporées dans les fichiers PDF et DOC ne seront pas analysées pour détecter des données sensibles.
- Les fichiers doivent faire moins de 10 Mo.
- La prise en charge des types de fichiers suivants est disponible :
  - PDF
  - DOC(X)
  - TXT
  - XLS
  - CSV

Configurer des Détection de données schémas

Configurez un modèle et passez en revue les Détection de données modèles actuels. Un Détection de données modèle définit l'expression régulière utilisée pour faire correspondre les données à une table cible.

Avant de commencer

Rôle requis : data_discovery_admin

Procédure

1. Accédez à la **Sécurité de système** > **Découverte de données** > **Tous les schémas de données**.
2. Dans la Détection de données liste Modèle, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de Détection de données tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détection de données Champs des tâches

Champ	Description
Périmètre interne	Périmètre du modèle.
Description	Description de la tâche.
Nom	Nom du modèle de données.
Application	Périmètre de l'application du modèle.
Expression	Expression régulière utilisée pour découvrir le modèle de données. **Remarque :** La longueur de l'expression doit être inférieure à 1 000 caractères.
Mot clé (facultatif)	Un mot spécifique (ou des mots séparés par une virgule) à rechercher autour d'une expression. Doit être utilisé avec la **proximité des mots clés** **Remarque :** Un mot clé peut être utilisé pour rechercher un contexte supplémentaire pour un modèle. Par exemple, l'utilisation d'un mot clé peut aider à faire la différence entre une date de naissance ou une date d'embauche étant donné qu'ils ont le même formatage MM/JJ/AA.
Proximité des mots clés (facultatif)	À quelle distance de l'expression rechercher des mots clés. Doit être utilisé avec **le mot clé** **Remarque :** La valeur par défaut est 30, limite supérieure de 64
Configuration de la technique de confidentialité	Technique de confidentialité utilisée pour le modèle
Valeur synthétique	Liste des valeurs substituées aux schémas
Type	Type de modèle ○ **Local** : le modèle est basé sur regex ○ **Modèle** : utilise le service AI/ML

4. Sélectionnez **Soumettre**.
   - Le bouton **Test** vous permet de tester votre expression régulière avant de soumettre la liste de modèles de données.

Le modèle de données doit être défini comme actif pour être utilisé avec les travaux planifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Accédez à la **Sécurité de système** > **Découverte de données** > **Schémas de données actifs**.
6. Dans la liste Modèle Détection de données actif, sélectionnez **Modifier**.
7. Sélectionnez la liste de modèles dans les **listes disponibles** et déplacez-la vers **Listes sélectionnées**.

Schémas de données par défaut

Passez en revue les expressions régulières du modèle de données par défaut incluses dans Détection de données. Ces schémas de données par défaut peuvent être utilisés pour filtrer des entrées de table en vue d'une classification ultérieure.

Les modèles par défaut suivants sont disponibles pour la découverte de données.

Nom	Description	Expression régulière	Mots clés	Exemples
Âge	Âge d'une personne entre 0 et 99 ans	\b([0-9]|[1-9][0-9]| 1[012][0-9])\b	âge	**Correspondant à** 24 **Ne correspondant pas** • 103 • -2
Date de naissance	Date de naissance au format JJ/MM/AAAA	\b[0-3] ? [0-9]/ [0-3]? [0-9]/(?:[0-9]{2})? [0-9]{2}\b	date de naissance, date de naissance, date de naissance	**Correspondant à** • 06/18/2012 • 1/1/19
E-mail	Adresse e-mail standard	\b[\w !#$ %&'* +/= ?'{|}~^-]+(?:\. [\w !#$ %&'* +/= ?'{|}~^-]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b		**Correspondant à** • johndoe@emailserver.com • historyprofessor@college **Ne correspondant pas** • notanemail.com • bademail@.org
Numéro d'identification du véhicule	Un numéro d'identification de véhicule (NIV)	\b[A-HJ-NPR-Z0-9]{17}\b		**Correspondant à** AHUYA31581L000000
Adresse IP	Adresse IP standard	**IP à 4 chiffres** \b(?:(?:25[0-5]| 2[0-4][0-9]|		**IP à 4 chiffres correspondante** 102.28.46.103 **IP à 6 chiffres correspondante**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description	Expression régulière	Mots clés	Exemples
		[01]? [0-9] [0-9]?)\.) {3} (?:25[0-5]| 2[0-4] [0-9]| [01]? [0-9] [0-9]?)\b **IP à 6 chiffres** \b(((?: [0-9A-Fa-f] {1,4} (?:: [0-9A-Fa-f] {1,4})*) ?) :: ((?: [0-9A-Fa-f] {1,4} (?:: [0-9A-Fa-f] {1,4})*) ?))| ((?: [0-9a-fA-F] {1,4}:) {7} [0-9a-fA-F] {1,4})\b		914b :d45a :61ea :6346:59bc :30
Carte de crédit : Visa	Numéro de carte de crédit Visa	\b4[0-9]{12}(?: [0-9]{3}) ?\b		**Correspondant à** 4444434342424242
Carte de crédit : American Express	Numéro de carte de crédit American Express	\b3[47][0-9]{13}\b		**Correspondant à** 378225246366005
Carte de crédit : Mastercard	Numéro de carte de crédit Mastercard	\b(?:5[1-5][0-9]{2}| 222[1-9]|22[3-9] [0-9]|2[3-6][0-9] {2}|27[01][0-9]| 2720)[0-9]{12}\b		**Correspondant à** 5555444455554444
Carte de crédit - Diners Club	Numéro de carte de crédit Diners Club	\b3(?:0[0-5]|[68] [0-9])[0-9]{11}\b		**Correspondant à** 3056930009020004

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description	Expression régulière	Mots clés	Exemples
Carte de crédit : Discover	Numéro de carte de crédit Discovery	\b6(?:011|5[0-9]{2})[0-9]{12}\b		**Correspondant à** 6011025690875424
Carte de crédit : CCV	Numéro de sécurité de la carte de crédit	\b[0-9]{3,4}\b	cvv,code de vérification,code de sécurité	**Correspondant à** 124
Carte de crédit : date d'expiration	Expiration de la carte de crédit au format MM/AAAA	\b(([1-9])|(0[1-9]|1[0-2]))\/ ? ([0-9]{4}|[0-9]{2})\b	expirer, exp	**Correspondant à** • 02/2027 • 04/23 **Ne correspondant pas** 03/9
États-Unis – Numéro de sécurité sociale	Numéro de sécurité sociale de citoyen américain	\b(?! 666|000|9\d{2})\d{3}-(?! 00)\d{2}-(?! 0{4})\d{4}\b		**Correspondant à** 001-22-111
États-Unis - Numéro de téléphone	Numéro de téléphone aux États-Unis **⚠ Avertissement :** N'utilise pas l'indicatif d'appel des États-Unis.	\b\(?([0-9]{3})\)? [-.]? ([0-9]{3})[-.]? ([0-9]{4})\b		**Correspondant à** 2065550199 **Ne correspondant pas** 1 555 238 0199
États-Unis - Numéro de passeport	Numéro de passeport américain à 9 chiffres	\b[a-zA-Z0-9]\d{8}\b		**Correspondant à** 770022122
États-Unis - ID de contribuable	Numéro d'identification de contribuable américain	\b(9\d{2})([\-] ?)([7]\d|8[0-8])([\-]?)(\d{4})\b		**Correspondant à** 927 70 5828
Numéro de permis de conduire de l'État de Californie	Numéro de permis de conduire de l'État de Californie, États-Unis	\b[a-zA-Z]\d{7}\b		**Correspondant à** A0002144
USA – Numéro de routage bancaire	Numéro d'acheminement bancaire des États-Unis (ABA)	\b((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|(6[1-9])|(7[0-2])|80)([0-9]{7})\b		**Correspondant à** 125210305

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la Détection de données table cible

Ajoutez une cible des tables à utiliser dans les Détection de données tâches. Seules les tables cibles seront analysées pour les schémas de données.

Avant de commencer
Rôle requis : data_discovery_admin

Pourquoi et quand exécuter cette tâche
Lorsqu'une Détection de données tâche est exécutée, elle s'exécute sur toutes les tables cibles avec tous les schémas actifs.

Procédure

1. Sélectionner **Sécurité de système** > **Découverte de données (classique)** > **Tables cibles**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez votre table cible dans le champ **Nom de table** .
4. Sélectionnez **Soumettre**.

Activer des tâches parallèles pour Détection de données

Utilisez des tâches parallèles pour réduire le temps d'exécution de vos Détection de données tâches.

Avant de commencer
Rôle requis : admin

Procédure
Par défaut Détection de données , les tâches sont exécutées à l'aide d'un seul thread. Plusieurs threads peuvent être activés pour Détection de données les analyses complètes.

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Créer la propriété `com.glide.data_discovery.max_concurrent_item_workers`
3. Vérifiez que le **type** est un nombre entier.
4. **Important :**
   Il est recommandé de commencer avec un petit nombre de travailleurs par nœud (2 ou 3).

   Saisissez le nombre d'agents parallèles dans le champ **Valeur** jusqu'à 5.

Détection de données rôles

Vous pouvez affecter des Détection de données rôles pour limiter l'accès des utilisateurs à certains types de données.

Administrateur de la découverte des données [sn_data_discovery.data_discovery_admin]

Affichez, créez et modifiez des schémas de données et des tâches connexes.

- Schémas de données :
  - Créer
  - Lecture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Mettre à jour
- Supprimer

- Schémas de données actifs :
  - Supprimer
  - Lire
- Emplois:
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer
  - Planifier
  - Mettre en pause
  - Reprendre
  - Annuler
- Tables cibles :
  - Créer
  - Lire
  - Écriture
- Configuration granulaire :
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer
- Résultats granulaires :
  - Créer
  - Lire
  - Actions

> **Remarque :**
> Les utilisateurs disposant de ce rôle peuvent uniquement effectuer l’action Ignorer

Contient des rôles

Liste des rôles contenus dans le rôle.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Les administrateurs sont automatiquement affectés à ce rôle lors de l'installation du produit.

Remarque :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

Auditeur de découverte de données [sn_data_discovery.data_discovery_auditor]

Lire les schémas de données et les tables cibles.

- Lire des schémas de données
- Lire les schémas de données actifs
- Lire les Détection de données tâches
- Lire les tables cibles
- Examiner la configuration granulaire
- Examiner les résultats granulaires

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Aucun.

Administrateur de classification des données [data_classification_admin]

Lisez les schémas de données, les tâches de découverte et la table data_classification lorsqu'un résultat de modèle spécifique activé est classifié.

Contient des rôles

Le rôle de classification des données contient la liste des rôles contenus dans le rôle data_classification_auditor.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Considérations spéciales

Remarque :
Pour plus d'informations sur le rôle administrateur de classification des données, reportez-vous à la section Installation de données de démonstration du module d'extension Classification des données.

Détection de données Résultats des tâches

La Détection de données page Résultats affiche les détails des données trouvées par une tâche. Vous pouvez utiliser la page Résultats pour examiner les résultats d'une tâche et commencer à classer des données.

La Détection de données page Conclusions affiche les détails suivants après une tâche terminée.

Colonne	Description
Entrée du dictionnaire	Colonne de la table cible où les données ont été
Table	Table cible dans laquelle les données ont été trouvées
Modèle de données	Modèle de données utilisé pour trouver les données
Nombre de correspondances de modèles de données	Nombre d'entrées de données qui correspondent au modèle de données
Nombre total d'analyses de lignes	Nombre de lignes analysées pendant la tâche
Pourcentage de lignes correspondantes	Pourcentage de lignes dans la table cible qui correspondent au modèle de données
Détection de données Travail	Tâche utilisée sur la table cible
Statut	État de l'entrée

Après l'exécution d'une Détection de données tâche, les résultats affichent l'état Nouveau. Si aucune action n'est nécessaire, vous pouvez laisser les données tranquilles, ce qui définit automatiquement l'état sur Ignoré. Sinon, vous pouvez classer les données, par exemple en créant des classifications de données définies par l'utilisateur, pour les préparer à l'anonymisation des données à l'aide de l'outil Classification des données .

Résultats granulaires

Les utilisateurs peuvent sélectionner l'action **Suivre les résultats granulaires** pour utiliser la Résultats granulaires page afin de prendre des mesures sur des enregistrements détectés spécifiques. Consultez Résultats granulaires pour plus d'informations.

Protections disponibles

Sélectionnez le bouton **Protections disponibles** pour examiner le service de contrôle des entrées, l'état, les notes et le dernier enregistrement. À partir de Xanadu cette fonctionnalité, seul Chiffrement de champ.

Les services Protecton sont également accessibles depuis le tableau de bord. Pour en savoir plus sur le tableau de bord, reportez-vous à la section Détection de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consolider les résultats

Les résultats des tâches peuvent être consolidés à l'aide du bouton **Consolider les résultats** . Les résultats de tâche partagés entre deux tâches distinctes seront ensuite consolidés sous la tâche exécutée le plus récemment.

Remarque :
Seules les tâches d'analyse complète terminées peuvent être consolidées

Classer les données dans la page des résultats de tâche Détection de données

Classez les données directement à Détection de données partir de la page de résultats d'une tâche.

Avant de commencer
Rôle requis : data_discovery_admin et admin

Une tâche doit terminer une exécution réussie avant qu'une donnée de résultat puisse sembler classifiée.

Procédure

1. Accéder à **Sécurité de système** > **Découverte de données** > **Tâche de découverte de données**.
2. Sélectionnez l'entrée que vous souhaitez classer.
3. Dans la Détection de données liste Résultats, sélectionnez **Classifier**.
4. Sélectionnez les classifications de données que vous souhaitez associer aux entrées de table.
5. Sélectionnez **Classifier**.

Détection de données Types de données pris en charge

Vérifiez quels types de champs sont pris en charge lors de l'utilisation de Détection de données.

Remarque :
Tous les types de champs qui ont été classifiés ne sont pas disponibles pour Détection de données.

Certains types de champs à risque élevé sont désactivés par défaut, comme indiqué dans la table. Pour plus d'informations sur les champs, voir Types de champs .

Types de champs pris en charge pour la découverte de données

Type de champ	Disponible par défaut
audio	Non
condition	Non
condition_string	Non
currency	Oui
décimal	Oui
due_date	Oui
flottant	Oui
glide_date	Oui
glide_date_time	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de champ	Disponible par défaut
glide_duration	Non
glide_time	Oui
HTML	Non
icône	Non
entier	Oui
ip_addr	Non
ip_address	Non
journal	Oui
journal_input	Oui
journal_list	Oui
longint	Oui
name_values	Non
percent_complete	Non
phone_number_e164	Oui
prix	Oui
chaîne	Oui
string_full_utf8	Oui
translated_html	Non
translated_text	Non
URL	Non
user_image	Non
vidéo	Non
wiki_text	Non

Traduction automatique

Analyse avec configuration granulaire

L'analyse granulaire permet d'analyser des colonnes de table spécifiques en vue d'une découverte. Les tâches traditionnelles Détection de données analysent l'ensemble de la table pour découvrir les données, tandis que l'analyse granulaire cible des colonnes spécifiques de la table, offrant ainsi plus de contrôle sur le processus de découverte

Avant de commencer

Rôle requis : admin, sn_data_discovery_admin data_privacy_admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Découverte de données (classique)** > **Configuration granulaire**.
2. Dans la liste **Configurations granulaires** , sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire **Champs de configuration granulaire** .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de configuration granulaire

Champ	Description
Entrée du dictionnaire	Colonne à analyser.
Table	Table à analyser.
Étiquette de colonne	Étiquette de la colonne à analyser
Point de début de l'analyse	Les données sensibles ne seront découvertes que le jour du point de début de l'analyse et après celui-ci. **Remarque :** Si le point de début de l'analyse est laissé vide, toutes les entrées de la colonne sont analysées. Si le point de début de l'analyse est modifié, l'analyse sera réinitialisée pour commencer à partir de l'horodatage nouvellement configuré.
Actif	Cochez cette case pour activer la configuration granulaire.

4. Sélectionnez **Soumettre**.
   Les enfants des tables extensibles peuvent être sélectionnés pour la configuration.
5. **Facultatif :** Sélectionnez la configuration granulaire pour la table parente, sélectionnez **Sélectionner les tables enfants** et sélectionnez les tables enfants pour l'analyse.

Résultats

La colonne spécifique de la table cible sera analysée pour détection. L'analyse granulaire utilise les schémas de données des **schémas de données actifs**. Vous pouvez examiner les résultats et prendre des mesures à l'adresse suivante : **Tous** > **Sécurité de système** > **Découverte de données (classique)** > **Résultats granulaires**. Consultez Résultats granulaires pour plus d'informations.

Résultats granulaires

Les résultats granulaires peuvent être examinés à l'aide de l'outil Résultats granulaires.

Examen des résultats granulaires

Les résultats granulaires sont utilisés pour examiner jusqu'à 500 résultats à partir de configurations granulaires. Lorsqu'il y a 500 résultats, l'analyse des configurations granulaires est suspendue jusqu'à ce qu'une action soit effectuée.

Étiquette de colonne	Description
Enregistrement	Enregistrement détecté.
Table	Table parente de l'enregistrement.
Colonne	Colonne de l'enregistrement où des informations sensibles ont été découvertes.
Schémas de données	Modèle utilisé pour détecter l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de colonne	Description
Action	Action à effectuer sur les résultats. Sélectionnez cette option pour modifier **Important :** Le rôle data_privacy_admin est requis pour effectuer l'action d'anonymisation sur un enregistrement. **Revue** L'enregistrement est en attente de révision. Elle est affectée aux nouvelles découvertes granulaires. **Ignorer** Aucune action ne sera effectuée sur l'enregistrement **Anonymiser** L'enregistrement est anonymisé.
Statut	État de l'enregistrement. **Nouveau** État affecté au résultat lorsqu'il est signalé pour la première fois **Traité** Lorsque l'action choisie par l'utilisateur a été appliquée avec succès au résultat **Remarque :** Les résultats traités sont stockés pendant 3 jours dans la table des résultats granulaires avant la suppression **Revue manuelle** Lors de l'application, l'action choisie par l'utilisateur a échoué. **Avertissement :** Les résultats de l'examen manuel doivent être supprimés par les utilisateurs après avoir pris les mesures appropriées.

Avertissement : La restauration n'est pas prise en charge pour l'anonymisation déclenchée à partir des résultats granulaires.

Découverte contextuelle

Utilisez la découverte contextuelle pour détecter les données sensibles qui ne suivent pas des schémas fixes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La découverte de données prend en charge l'utilisation d'un modèle de reconnaissance d'entité nommée (NER) pour détecter des données telles que des noms, des organisations, des nationalités et des affiliations politiques. Les schémas de données de type **Modèle** utilisent cette fonctionnalité, voir type de modèle dans Configurer des Détection de données schémas pour plus de détails.

⚠ Avertissement :
Cette fonctionnalité nécessite une vérification de licence de la part du client avant d'être activée.

La découverte basée sur les modèles IA prend en charge 5 modèles par défaut.

Modèles de découverte contextuelle

Schéma	Description	Texte d'exemple	Texte correspondant
Personne	Nom de la ou des personnes	John Doe est venu prendre un café.	John Doe
Nationalité, groupes religieux ou politiques (PNR)	Affiliations nationales, religieuses et politiques.	C'était un Américain.	Américain
Emplacement	Adresses ou informations sur l'emplacement	Il était à New York	New York
Date_Time	Informations sur les dates et l'heure	Il est venu à 9h30 aujourd'hui.	9:30 aujourd'hui
Organisation	Noms des organisations	Il travaille chez ServiceNow.	ServiceNow

ℹ Remarque :
La découverte basée sur les modèles IA ne prend en charge que l'anglais à utiliser avec Anonymisation en temps réel(RTA) pour les tables et le canal Data Kit.

Politiques Détection de données

Utilisez Détection de données des politiques pour analyser des tables spécifiques et activer les tâches basées sur les colonnes.

Détection de données Les politiques vous permettent d'avoir un contrôle précis sur la définition de schémas de données, de tables et de colonnes spécifiques qui doivent être inclus dans une tâche. En outre, l'utilisation de politiques vous permet de créer plusieurs paramètres de tâche de découverte en même temps, au lieu d'une configuration globale. Vous pouvez examiner vos Détection de données politiques en accédant à **Tous** > **Sécurité de système** > **Découverte de données (classique)** > **Politiques de découverte de données**.

ℹ Remarque :
Si aucune colonne n'est sélectionnée pour une politique, toutes les colonnes de la table cible sont analysées

Reportez-vous à la section Créer une Détection de données politique pour savoir comment créer une Détection de données politique.

Créer une Détection de données politique

Créez une Détection de données politique pour un contrôle granulaire sur vos Détection de données tâches.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin, sn_data_discovery_admin data_privacy_admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Découverte de données (classique)** > **Politiques de découverte de données**.
2. Sélectionnez le bouton **Nouveau** .
3. Remplissez le formulaire.

Politique de découverte de données

Étiquette	Description
Nom	Nom de la politique
Colonne(s) cible(s)	Sélectionner les colonnes cibles à utiliser dans la politique **Remarque :** Si aucune colonne n'est sélectionnée, toutes les colonnes de la table cible sont analysées
Table cible	Sélectionner la table cible à utiliser dans la politique
Actif	Détermine si la politique est active ou inactive **Remarque :** La valeur par défaut est active
Modèle de données	Le modèle de données que la politique utilisera.

4. Sélectionnez **Soumettre**.

Résultats
Sélectionnez la politique lors de la création d'un Détection de données Emplois.

Détection de données Boutique

Détecter et suivre les données sensibles au sein d'une instance ServiceNow

Magasin de découverte de données

Utilisez cette fonction Détection de données pour détecter les données sensibles au sein de votre instance. Recherchez des données sensibles structurées telles que les numéros de carte de crédit, les numéros de téléphone, les numéros de sécurité sociale (SSN), etc. Lancez-vous rapidement en utilisant des schémas de données courants prêts à l'emploi ou créez les leurs pour une expérience plus granulaire. Pour les données sensibles non structurées et souvent contextuelles telles que les noms, adresses, etc., vous pouvez utiliser l'IA et l'apprentissage machine pour faciliter l'identification

Détection de données Vue d'ensemble du magasin

Obtenez une vue d'ensemble de vos mesures de découverte de données et un point de départ pour l'utilisation de ses outils.

Détection de données politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Passez en revue les politiques actuelles de découverte des données et configurez-les.

Sources Détection de données

Voir les schémas de données et les tables cibles actuellement utilisés par vos tâches de découverte

Détection de données Découverte planifiée

Planifiez et examinez les tâches de découverte, y compris les tâches de découverte de colonnes granulaires.

Détection de données Vue d'ensemble du magasin

Obtenez une visibilité sur les données sensibles de votre instance et travaillez à la mise en œuvre de mesures de sécurité pour éviter la perte ou l'exposition de données sensibles.

L'onglet **Vue d'ensemble** fournit un point de départ facile pour utiliser la découverte de données, tout en affichant les mesures et résultats de découverte importants. Accédez à la **Tous** > **Découverte de données** > **Vue d'ensemble** pour commencer à utiliser l'onglet.

Créer une politique de découverte et planifier la tâche de découverte

Vous pouvez commencer à utiliser Détection de données avec les éléments d'action recommandés. Sélectionnez **Créer une politique** pour définir les schémas de données sensibles à identifier et la manière dont ils doivent être traités. Reportez-vous à la section Détection de données politique pour plus d'informations sur la création d'une nouvelle politique. Sélectionnez **Planifier une tâche** pour planifier des tâches de découverte de données qui analyseront votre instance à la recherche d'informations sensibles. Voir Détection de données Découverte planifiée pour plus d'informations sur la planification d'une nouvelle tâche de découverte.

Résumé de la découverte de données

Vous pouvez consulter en un coup d'œil les mesures importantes Détection de données . En outre, vous pouvez sélectionner les graphiques à explorer plus en détail. Pour plus d'informations sur l'examen des résultats de découverte, reportez-vous à Examiner les résultats de découverte.

Données découvertes

Histogramme superposant les classifications et la quantité de données détectées. Il résume où et combien d'instances de PII ont été découvertes dans différentes tables de votre instance, classées par types de modèles de données.

Statut de découverte

Graphique en anneau affichant les proportions de l'état actuel de tous les modèles détectés, qu'il s'agisse de nouveaux résultats en attente d'examen, classés ou marqués comme ignorés

Données découvertes et tâches récentes

Vous pouvez passer en revue les données récemment découvertes et les tâches de découverte récentes dans cette section. Pour un examen plus détaillé de ces tableaux et de leur contenu, voir Détection de données Découverte planifiée

.

Détection de données politique

Utilisez Détection de données des politiques pour définir les schémas de données sensibles à identifier et la manière dont ils doivent être traités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'onglet **Politique** de passe en revue les politiques de Détection de données détection actuelles. Affichez les détails supplémentaires d'une politique en sélectionnant le bouton **Afficher les détails** . Modifiez, supprimez et changez l'état des politiques actuelles en sélectionnant les trois points . Pour créer une nouvelle politique, reportez-vous à Créer une nouvelle politique.

Créer une nouvelle politique

Créez une Détection de données politique pour commencer à analyser les tables à la recherche de schémas de données.

Avant de commencer

Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Politique**.
2. Sélectionnez le bouton **Créer une politique** .

   Modifiez ou supprimez une politique existante en sélectionnant l'icône extensible .
3. Renseignez les champs de la fenêtre contextuelle.

Nouveau formulaire de politique de découverte

Champ	Description
Nom	Saisissez un nom unique pour la politique.
Schémas de données	Sélectionnez les schémas de données sensibles à analyser. Vous pouvez sélectionner plusieurs schémas de données **Remarque :** Les schémas de données basés sur des modèles AI/ML nécessitent une licence supplémentaire et sont soumis à des termes et conditions supplémentaires.
Sélectionner des tables et des colonnes utilisateur	Vérifier la ou les tables à analyser **Remarque :** Toutes les colonnes de table sélectionnées seront analysées par défaut. Suivez l'étape ci-dessous pour restreindre votre sélection à des colonnes spécifiques
Tables et colonnes sélectionnées	Affiche une liste des tables et colonnes actuellement sélectionnées pour la politique

4. **Facultatif :** Sélectionner la flèche Une icône de permet d'afficher et de sélectionner des colonnes spécifiques de la table.
5. Sélectionnez **Enregistrer**.

Résultats

Par défaut, la nouvelle politique sera définie sur **Actif**. Sélectionnez l'icône extensible sélectionnez **Désactiver la politique**/Activer la **politique** pour changer son état.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sources Détection de données

Créez et sélectionnez les schémas de données à utiliser dans Détection de données, ainsi que les tables à analyser.

L'onglet **Sources** vous aide à examiner tous vos schémas de Détection de données données, à définir le modèle à utiliser pour les analyses et à sélectionner les tables à analyser.

Tous les schémas

La table **Tous les schémas** répertorie tous les modèles actuels. Notez que les modèles inactifs apparaîtront dans cette liste. Reportez-vous à la section Créer un nouveau modèle de données pour créer un nouveau modèle de données.

Remarque :
Les modèles doivent être actifs pour être utilisés dans les tâches de découverte.

Table Tous les schémas

Étiquette	Description
Nom	Nom du modèle de données.
Expression	Expression régulière utilisée pour découvrir le modèle de données.
Mot clé	Un mot spécifique (ou des mots séparés par une virgule) à rechercher autour d'une expression.
Proximité des mots clés	À quelle distance de l'expression rechercher des mots clés.
Configuration de la technique de confidentialité	Technique de confidentialité utilisée pour le modèle

Schémas actifs

La table **Schémas actifs** répertorie tous les schémas de données actifs actuels. Reportez-vous à la section Sélectionner des schémas de données actifs pour savoir comment définir un modèle sur actif et utilisé par les tâches de découverte.

Table Schémas actifs

Étiquette	Description
Nom	Nom du modèle de données.
Expression	Expression régulière utilisée pour découvrir le modèle de données.
Mot clé	Un mot spécifique (ou des mots séparés par une virgule) à rechercher autour d'une expression.
Proximité des mots clés	À quelle distance de l'expression rechercher des mots clés.
Configuration de la technique de confidentialité	Technique de confidentialité utilisée pour le modèle

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables cibles

La table **Tables cibles** répertorie toutes les tables actuellement sélectionnées pour les tâches de découverte. Reportez-vous à la section Sélectionner les tables cibles pour sélectionner des tables à utiliser dans les tâches de découverte.

Table de tables cibles

Étiquette	Description
Nom de la table	Le nom de la table
Nom complet	Nom d'affichage de la table (utilisé dans la génération de rapports)
Application	Le périmètre de l'application de la table.

Créer un nouveau modèle de données

Créez un nouveau Détection de données modèle de boutique.

Avant de commencer

Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Sources**.
2. **Sélectionnez Tous les modèles** dans le volet de navigation.
3. Sélectionnez le bouton **Créer** .
4. Remplissez le formulaire.

Formulaire Nouveau schéma de données

Champ	Description
Description	Description du modèle.
Nom	Nom du modèle de données.
Expression	Expression régulière utilisée pour découvrir le modèle de données. **Remarque :** La longueur de l'expression doit être inférieure à 1 000 caractères.
Mot clé	Un mot spécifique (ou des mots séparés par une virgule) à rechercher autour d'une expression. Doit être utilisé avec la **proximité des mots clés**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Un mot clé peut être utilisé pour rechercher un contexte supplémentaire pour un modèle. Par exemple, l'utilisation d'un mot clé peut aider à faire la différence entre une date de naissance ou une date d'embauche étant donné qu'ils ont le même formatage MM/JJ/AA.
Proximité des mots clés	À quelle distance de l'expression rechercher des mots clés. Doit être utilisé avec **le mot clé** **Remarque :** La valeur par défaut est 30, limite supérieure de 64
Configuration de la technique de confidentialité	Technique de confidentialité utilisée pour le modèle
Valeur synthétique	Liste des valeurs substituées aux schémas
Type	Type de modèle
Application	Périmètre de l'application du modèle.
Champ d'application	Périmètre du modèle.

5. **Facultatif :** Sélectionnez le bouton **Test** pour tester vos expressions régulières si nécessaire.
6. Sélectionnez **Soumettre**.

Résultats

Le nouveau modèle de données doit être défini comme actif pour être utilisé dans les tâches de découverte. Consultez Sélectionner des schémas de données actifs pour plus d'informations.

Sélectionner des schémas de données actifs

Sélectionnez les schémas de données actifs à utiliser pour Détection de données les tâches.

Avant de commencer

Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Sources**.
2. **Sélectionnez les modèles actifs** dans le volet de navigation.
3. Cliquez sur le bouton **Modifier**.
4. Vérifiez les schémas à activer, ils s'afficheront dans le côté droit de la fenêtre contextuelle.
5. **Facultatif :** Sélectionnez et faites glisser les modèles pour les réorganiser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

(Optional) L'ordre des schémas de données déterminera également l'ordre des techniques d'anonymisation appliquées pour l'anonymisation des schémas de données.

6. Sélectionnez le bouton **Enregistrer** .

Sélectionner les tables cibles

Sélectionnez les tables cibles à utiliser dans les tâches de découverte.

Avant de commencer
Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Sources**.
2. **Sélectionnez Tables cibles** dans le volet de navigation.
3. Cliquez sur le bouton **Modifier**.
4. Vérifiez les tables à cibler, elles s'afficheront dans le côté droit de la fenêtre contextuelle.

Remarque :
Les tables cibles analyseront toutes les colonnes, sauf indication contraire dans la politique.

5. Sélectionnez le bouton **Enregistrer** .

Résultats
Les tables sélectionnées vont maintenant être ciblées par les tâches de découverte planifiées.

Détection de données Découverte planifiée

Configurez et planifiez des tâches de découverte de données afin d'analyser votre instance à la recherche d'informations sensibles.

Tâches de découverte

La table **Tâches de découverte** répertorie toutes les tâches de découverte. Reportez-vous à la rubrique pour Créer une tâche de découverte créer une nouvelle tâche de découverte.

Table des tâches de découverte

Nom	Nom de la tâche
Description	La description de poste
Terminé (%)	Pourcentage d'achèvement de la tâche
Type d'analyse	Type d'analyse de la tâche. Les états possibles sont les suivants : • **Exemple** : Scanne 10 000 entrées. • **Complet** : analyse toutes les entrées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des tâches de découverte (suite)

Date de début	Date de début de la tâche
Mis à jour	Moment de la dernière mise à jour de la tâche.
État	État de la Détection de données tâche. Les états possibles sont les suivants : • **Prêt à planifier** : état par défaut des nouvelles tâches. • **Planifié** : l'exécution de la tâche est planifiée. • **En cours** : la tâche est en cours d'exécution. • **Terminé** : la tâche s'est terminée avec succès. • **Erreur** : la tâche a cessé de s'exécuter en raison d'une erreur. • **Annulé** : la tâche a été annulée. • **En pause** : la tâche est en pause.
Exécuter	Fréquence d'exécution planifiée de la tâche.

Résultats de découverte

La table **Résultats de découverte** répertorie tous les résultats découverts à partir des tâches de découverte. Consultez Examiner les résultats de découverte pour examiner et classer les résultats des tâches de découverte.

Table des résultats de découverte

Étiquette	Description
Entrée du dictionnaire	Colonne de la table cible dans laquelle se trouvaient les données
Table	Table cible dans laquelle les données ont été trouvées
Modèle de données	Modèle de données utilisé pour trouver les données
Nombre de correspondances de modèles de données	Nombre d'entrées de données qui correspondent au modèle de données
Nombre total d'analyses de lignes	Nombre de lignes analysées pendant la tâche
Pourcentage de lignes correspondantes	Pourcentage de lignes dans la table cible qui correspondent au modèle de données
Tâche de découverte de données	Tâche utilisée sur la table cible
Statut	État de l'entrée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration granulaire

La table **Configuration granulaire** répertorie toutes les tâches de découverte granulaire. Reportez-vous à la rubrique Créer une tâche granulaire pour savoir comment créer une tâche de découverte granulaire.

Table de configuration granulaire

Étiquette	Description
Table	Table de la tâche de découverte granulaire
Étiquette de colonne	Étiquette de colonne de la tâche de découverte granulaire
Point de début de l'analyse	Les données sensibles ne seront découvertes que le jour du point de début de l'analyse et après celui-ci. **Remarque :** Si le point de début de l'analyse est laissé vide, toutes les entrées de la colonne sont analysées.
Actif	État de la tâche de découverte granulaire.

Résultats granulaires

La table **Résultats granulaires** répertorie tous les résultats granulaires des tâches de découverte granulaire. Consultez Examiner les résultats granulaires pour examiner les résultats des tâches de découverte granulaire.

Table des résultats granulaires

Étiquette	Description
Enregistrement	Enregistrement détecté
Table	Table parente de l'enregistrement
Modèle de données	Modèle utilisé pour détecter l'enregistrement
Action	Action à effectuer sur l'enregistrement **Revue** L'enregistrement est en attente de révision. Affecté aux nouvelles découvertes granulaires **Ignorer** Aucune action ne sera effectuée sur l'enregistrement **Anonymiser** L'enregistrement est anonymisé
Statut	État de l'enregistrement **Nouveau** État affecté au résultat lorsqu'il est signalé pour la première fois

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des résultats granulaires (suite)

Étiquette	Description
	Traité Lorsque l'action choisie par l'utilisateur a été appliquée avec succès au résultat **Remarque :** Les résultats traités sont stockés pendant 3 jours dans la table des résultats granulaires avant la suppression **Revue manuelle** Lors de l'application, l'action choisie par l'utilisateur a échoué **Avertissement :** Les résultats de l'examen manuel doivent être supprimés par les utilisateurs après avoir pris les mesures appropriées.

Créer une tâche de découverte

Créez et planifiez une nouvelle tâche du magasin de découverte de données.

Avant de commencer
Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Découverte planifiée**.
2. Sélectionnez **Tâches de découverte** dans le volet de navigation de droite.
3. Remplissez le formulaire.

Planifier un nouveau formulaire de découverte

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Type d'analyse	Nombre d'entrées à analyser. Les états possibles sont les suivants : ○ **Exemple** : Scanne 10 000 entrées. ○ **Complet** : analyse toutes les entrées.
Sélectionner une police	La politique à utiliser pour la tâche planifiée.
Date de début	Définit la date de début de la tâche.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ce champ. L'heure saisie dans le champ **de début de la fenêtre de temps** doit être antérieure à l'heure saisie dans le champ de fin de la **fenêtre de temps** . **Remarque :** Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.
Fin de la fenêtre de temps	La fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute jusqu'à l'heure saisie dans ce champ. Si la tâche n'est pas terminée cette fois-ci, la tâche est interrompue et reprend au début de la fenêtre de temps suivante. L'heure saisie dans le champ **de fin de la fenêtre de temps** doit être postérieure à l'heure saisie dans le champ de début de la **fenêtre de temps** . **Remarque :** Une valeur de temps valide est le temps universel coordonné basé sur une notation de 24 heures.

4. Sélectionnez le bouton **Planifier** .

Examiner les résultats de découverte

Classer des données dans le magasin de découverte de données

Avant de commencer
Rôle requis : discovery.admin

Procédure

1. Accéder à **Tous** > **Découverte de données** > **Découverte planifiée**.
2. Sélectionnez **Résultats de découverte** dans le volet de navigation de droite.
3. Vérifiez les entrées à classer.
   Sélectionnez le bouton **Modifier** pour modifier la classification des entrées sélectionnées.
4. Sélectionnez le bouton **Classifier** .

   Remarque :
   Sélectionnez le bouton **Protections disponibles** pour passer en revue les options de protection des données classifiées.

5. Sélectionnez les classifications de données que vous souhaitez associer aux entrées de table.
6. Sélectionnez **Classifier**.

Résultats
Les données sélectionnées sont maintenant classifiées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une tâche granulaire

Analysez des colonnes de table spécifiques dans le magasin de découverte de données.

Avant de commencer
Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Découverte planifiée**.
2. Sélectionnez **Configuration granulaire** dans le volet de navigation de droite.
3. Sélectionnez **Créer**.
4. Remplissez le formulaire.

Formulaire Créer une configuration granulaire

Champ	Description
Table	Table à analyser
Étiquette de colonne	Colonne à analyser
Point de début de l'analyse	Les données sensibles ne seront découvertes que le jour du point de début de l'analyse et après celui-ci. **Remarque :** Si le point de début de l'analyse est laissé vide, toutes les entrées de la colonne sont analysées. Si le point de début de l'analyse est modifié, l'analyse sera réinitialisée pour commencer à partir de l'horodatage nouvellement configuré.

5. Définir **le curseur Actif** .
6. Sélectionnez **Enregistrer**.

Résultats
Une analyse granulaire est planifiée pour s'exécuter sur la table et la colonne cibles. Après son exécution, vous pouvez examiner les résultats de l'analyse.

Examiner les résultats granulaires

Examiner les résultats granulaires dans le magasin de découverte de données

Avant de commencer
Rôle requis : discovery.admin

Procédure

1. Accédez à la **Tous** > **Découverte de données** > **Découverte planifiée**.
2. Sélectionnez **Résultats granulaires** dans le volet de navigation de droite.
3. Examinez les entrées de table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de colonne	Description
Enregistrement	Enregistrement détecté.
Table	Table parente de l'enregistrement.
Schémas de données	Modèle utilisé pour détecter l'enregistrement.
Action	Action à effectuer sur les résultats. Sélectionnez cette option pour modifier **Important :** Le rôle data_privacy_admin est requis pour effectuer l'action d'anonymisation sur un enregistrement. **Revue** L'enregistrement est en attente de révision. Elle est affectée aux nouvelles découvertes granulaires. **Ignorer** Aucune action ne sera effectuée sur l'enregistrement **Anonymiser** L'enregistrement est anonymisé.
Statut	État de l'enregistrement. **Nouveau** État affecté au résultat lorsqu'il est signalé pour la première fois **Traité** Lorsque l'action choisie par l'utilisateur a été appliquée avec succès au résultat **Remarque :** Les résultats traités sont stockés pendant 3 jours dans la table des résultats granulaires avant la suppression **Revue manuelle** Lors de l'application, l'action choisie par l'utilisateur a échoué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de colonne	Description
	⚠ Avertissement : Les résultats de l’examen manuel doivent être supprimés par les utilisateurs après avoir pris les mesures appropriées.

⚠ Avertissement :

La restauration n'est pas prise en charge pour l'anonymisation déclenchée à partir des résultats granulaires.

Classification des données

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Explorer la classification des données



En savoir plus sur la classification des données.

Configurer la classification des données



Créez et configurez vos propres classes de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence pour la classification des données



Découvrez comment la classification des données fonctionne avec les données de démonstration.

Analyser les classifications des données



Apprenez à analyser les classifications de données.

Traduction automatique

Exploration de la classification des données

En savoir plus sur la classification des données.

Classification des données Active la prise en charge de :

- Visibilité des types de données hébergées sur une ServiceNow AI Platform instance.
- Respect des lois sur la protection de la vie privée et respect des exigences réglementaires pour les secteurs tels que les services financiers et la fabrication de dispositifs médicaux.

Classifications des données

La classification des données est un processus autonome dans lequel vous appliquez manuellement des classifications de données à des entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous classez les données selon ce que vous jugez approprié pour votre entreprise et vous pouvez modifier les classes de données disponibles si nécessaire.
- Lorsque vous classez des données, vous pouvez utiliser les classifications de données prédéfinies ou créer les vôtres. Bien que l'utilisation de classifications de données prédéfinies soit facultative, il est conseillé de le faire comme point de départ. Ces classifications de données prédéfinies sont incluses dans les données de démonstration que vous pouvez installer dans votre instance. Pour en savoir plus, reportez-vous aux

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sections Installation de données de démonstration du module d'extension Classification des données et Composants installés avec Classification des données des données de démonstration.

- Si vous créez vos propres classifications de données, vous pouvez également concevoir un système hiérarchique hiérarchisé avec des classifications de données parentes et enfants.

Tableau de bord de vue d'ensemble

Utilisez le tableau de bord Vue d'ensemble pour comprendre comment vos tables de données actuelles sont mappées à différentes classifications de données. Vous pouvez également analyser comment vos utilisateurs mondiaux, régionaux et internationaux peuvent avoir besoin de différentes approches de classification des données, en ce qui concerne l'utilisation ou l'accès aux données. Vous pouvez également personnaliser le contenu et la mise en page du tableau de bord de vue d'ensemble en fonction de vos besoins.

Pour apprendre à utiliser les API scriptées et REST disponibles pour appliquer les métadonnées de classification dans les processus, workflows et applications existants, consultez les rubriques suivantes :

- Classification des données : API REST
- DCManager : global
- ScopedDCManager : dans le champ d'application

Remarque :
Classification des données prend en charge Séparation de domaine et la table data_classification elle-même est séparée par processus.

Cas d'utilisation

Le Règlement général sur la protection des données (RGPD) est un règlement de l'Union européenne dont l'objectif est de permettre aux individus de contrôler leurs propres données personnelles. Vous pouvez utiliser des classifications de données, telles que les informations personnellement identifiables, pour identifier où les données personnelles sont stockées dans votre instance. En appliquant les mécanismes de sécurité appropriés pour protéger ces données personnelles contre les fuites, votre organisation répond aux exigences du RGPD.

Si vous stockez des informations sur les clients dans le , utilisez le code de classification des informations personnellement identifiables (PII) lorsque cela est nécessaire pour suivre les données soumises à la réglementation des lois locales sur la ServiceNow AI Platform confidentialité. Lorsque vous installez des données de démonstration, ce code de classification est automatiquement appliqué à certains champs sensibles à la sécurité de la table Utilisateur [sys_user]. Pour en savoir plus, consultez :

- Composants installés avec Classification des données des données de démonstration
- Affectation de classifications de données à des entrées de dictionnaire

Vous pouvez appliquer une classification de données restreinte aux colonnes de la table Employé qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (NSS). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté les classifications de données aux bonnes colonnes. Ils peuvent également afficher les détails de classification pour les types d'informations restreints.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installation de données de démonstration du module d'extension Classification des données

Lorsque vous effectuez une mise à niveau ou installez Yokohama (et une version ultérieure), le module d'extension Classification des données (com.glide.data_classification) est automatiquement activé. Toutefois, vous devez installer manuellement les données de démonstration fournies avec le module d'extension. Il comprend plusieurs classifications de données prédéfinies importantes, et il affecte également l'une d'entre elles à des colonnes de table Utilisateur spécifique [sys_user] dans votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Que vous installiez ou non des données de démonstration, le module d'extension activé Classification des données ajoute les rôles d'utilisateur suivants dans votre instance :

- data_classification_admin : peut administrer tous les aspects de l'application, y compris la Classification des données configuration et l'affectation de la classification des données.
- data_classification_auditor : peut auditer Classification des données les affectations de code effectuées dans les tables et les colonnes des utilisateurs.

Important :

Avis concernant l'utilisation par les Clients :

Toutes les décisions relatives à la mise en œuvre de la présente application sont à la seule discrétion du Client. Les clients reconnaissent et acceptent que l'utilisation de l'application ne constitue pas une déclaration par ServiceNow de la conformité à une loi ou à une réglementation et que toute langue, tout champ ou toute classification suggérés prêts à l'emploi fournis avec l'application ne constitue pas un avis juridique de ServiceNow.

Les Clients demeurent seuls responsables du respect de leurs obligations légales en vertu de la législation applicable, y compris (mais sans s'y limiter) la protection des données, les exigences de sécurité et les lois sur la protection de la vie privée, et sont responsables de la configuration et de l'apport de toutes les modifications nécessaires à cette application, y compris (mais sans s'y limiter) les modèles, pour répondre aux exigences des Clients.

Procédure

1. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.
2. Trouvez le module d'extension à l'aide Classification des données des critères de filtre et de la barre de recherche.
   Un message Installé s'affiche une fois que vous avez localisé le module d'extension.
3. Cliquez sur l'icône avec trois points verticaux, puis sélectionnez **Réparer** pour accéder à la boîte de dialogue Activer le module d'extension.
4. Sélectionnez **Charger les données de démonstration**, puis cliquez sur **Réparer**.

Composants installés avec Classification des données des données de démonstration

Lorsque vous installez les données de démonstration incluses dans le module d'extension Classification des données (com.glide.data_classification), plusieurs types de composants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sont installés dans votre instance. Ces composants comprennent des classifications de données prédéfinies et des affectations de code pour des colonnes d'utilisateur [sys_user} spécifiques.

Classifications des données installées

Classification des données	Description
Confidentiel	Données sensibles qui, si elles sont compromises, pourraient avoir un impact négatif sur les opérations.
Interne	Données internes non destinées à être divulguées au public.
Informations personnellement identifiables	Également connu sous le nom d'IPI. Données qui pourraient potentiellement être utilisées pour identifier une personne en particulier.
Public	Données qui peuvent être librement divulguées au public.
Restreint	Données d'entreprise hautement sensibles qui, si elles étaient compromises, pourraient exposer l'organisation à un risque financier ou juridique.

Classification des données Affectations

Table	Colonne affectée	Classification des données affectée
sys_user	code postal	Informations personnellement identifiables
sys_user	first_name	Informations personnellement identifiables
sys_user	E-mail	Informations personnellement identifiables
sys_user	city	Informations personnellement identifiables
sys_user	middle_name	Informations personnellement identifiables
sys_user	rue	Informations personnellement identifiables
sys_user	mobile_phone	Informations personnellement identifiables
sys_user	last_name	Informations personnellement identifiables
sys_user	pays	Informations personnellement identifiables
sys_user	sexe	Informations personnellement identifiables
sys_user	nom	Informations personnellement identifiables
sys_user	photo	Informations personnellement identifiables
sys_user	État	Informations personnellement identifiables
sys_user	home_phone	Informations personnellement identifiables

Création de classifications des données

Créez vos propres classifications de données définies par l'utilisateur dans la Classification des données table [data_classification] que vous pouvez ensuite affecter à des colonnes spécifiques dans des tables spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : data_classification_admin, admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Classification des données** > **Classes de données**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom de classification	Nom de la classification des données.
Description	Description de la classification des données.
Parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas parente de classifications de données enfants.
Application	Périmètre de l'application pour cette classification des données.

4. Si cette classification de données doit être parente de classifications de données enfants, cliquez sur **Nouveau**.
   Si vous ne souhaitez pas créer de classifications de données enfants, ignorez cette étape.
5. Renseignez les champs du formulaire.

Titre

Champ	Description
Nom de classification	Nom de la classification des données enfants.
Description	Description de la classification des données enfants.
Parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas parente de classifications de données enfants.
Application	Périmètre de l'application pour cette classification de données enfants.

6. Cliquez sur **Envoyer**.

Affectation de classifications de données à des entrées de dictionnaire

Affectez des classifications de données à des colonnes de table spécifiques dans la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, cela crée des entrées dans la table Classe de données de dictionnaire [m2m_dictionary_dataclass], que vous pouvez ensuite passer en revue dans le tableau de bord Vue d'ensemble.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : data_classification_admin et admin

Procédure

1. Dans le volet Navigateur, saisissez `sys_dictionary.list`.
2. Dans Entrées du dictionnaire, sélectionnez chacun des éléments auxquels vous souhaitez affecter des classifications de données spécifiques.
3. Après avoir sélectionné les éléments, cliquez sur **Actions sur les lignes sélectionnées**, puis sélectionnez **Classer**.

   Remarque :
   Pour effacer les classifications de données précédemment affectées pour les éléments de dictionnaire sélectionnés, vous pouvez sélectionner **Effacer la classification**.

4. Lorsque la boîte de dialogue Affecter à la classe de données s'affiche, sélectionnez les classifications de données que vous souhaitez affecter aux éléments de dictionnaire sélectionnés, puis cliquez sur **Classer**.

   Avertissement :
   Cela écrasera toutes les classifications existantes pour les éléments de dictionnaire sélectionnés.

   Vous pouvez sélectionner plusieurs classifications de données selon vos besoins.

   Consultez Data dictionary tables pour plus d'informations.

Analyse des classifications de données à l'aide du tableau de bord de vue d'ensemble

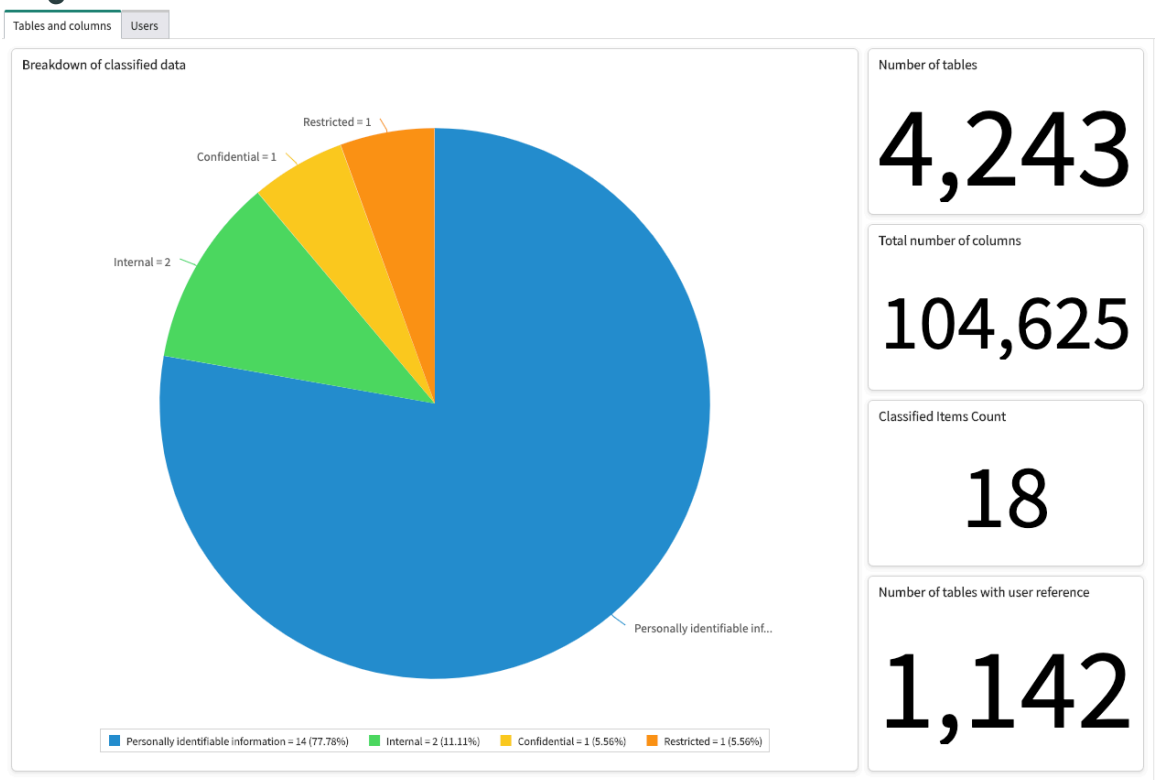
Le tableau de bord Vue d'ensemble présente l'état actuel des classifications de données au sein de votre instance et la façon dont vos utilisateurs sont répartis par emplacement.

Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez visualiser la sensibilité actuelle des données d'instance, ce qui contribue à accroître la sécurité et la conformité avec les lois sur la confidentialité. En utilisant le champ Emplacement dans les enregistrements utilisateur, les administrateurs mappent les utilisateurs dans différentes régions qui ont des réglementations de confidentialité différentes.

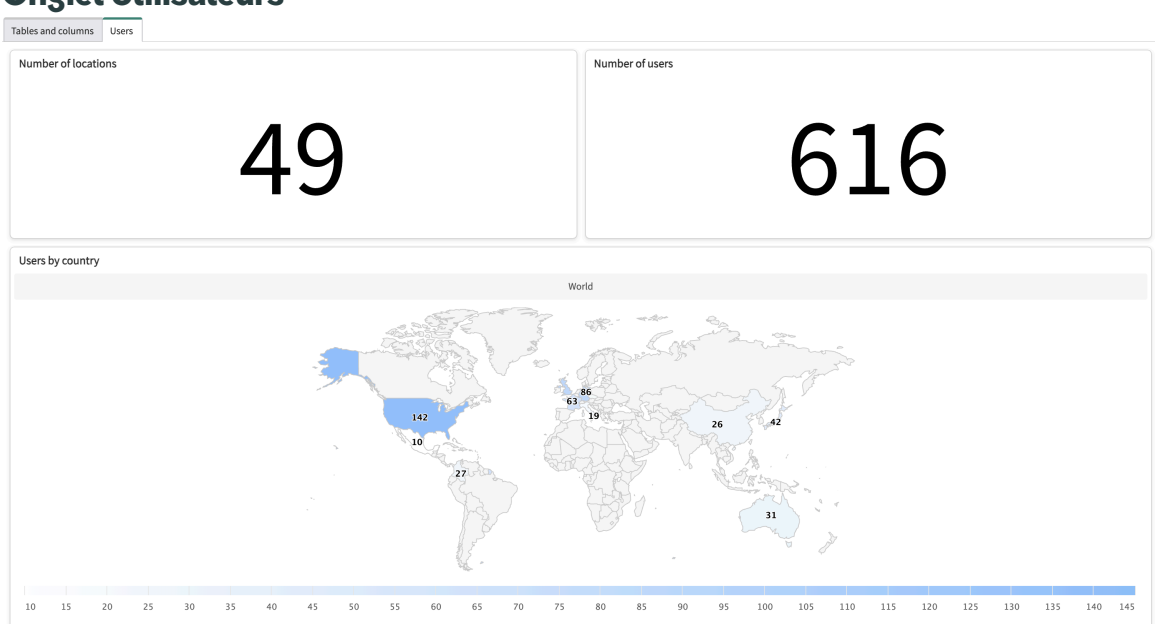
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Tables et colonnes



Onglet Utilisateurs



Rôles ServiceNow AI Platform requis

- data_classification_admin : administre tous les aspects de l'application, y compris la classification des données, la configuration et l'affectation Classification des données .
- data_classification_auditor : Audite Classification des données les affectations de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation

Pour obtenir d'autres exemples sur la façon dont différentes personnes de votre organisation utilisent ce tableau de bord, reportez-vous à la section Cas d'utilisation dans Classification des données.

Utilisateur	Utilisation du tableau de bord
data_classification_admin	Confirmez que vous avez affecté les classifications de données aux champs corrects dans votre instance.
data_classification_auditor	Vérifiez la sénilité et la sécurité des données dans votre instance.

Rapports

Titre	Type	Table source	Description
Répartition des données classées	Couronne	m2m_dictionary_dataclass	Fournit une répartition des classifications de données d'instance, par classe de données, total affiché au centre.
Nbre total de tables	Score unique	sys_dictionary	Nombre total de tables de données dans l'ensemble du dictionnaire.
Colonnes Total	Score unique	sys_dictionary	Nombre total de colonnes de données classifiées dans l'ensemble du dictionnaire.
Colonnes de référence de l'utilisateur	Score unique	sys_dictionary	Nombre total de colonnes de référence utilisateur dans le dictionnaire.
Nombre d'emplacements de l'utilisateur	Score unique	sys_user	Nombre total d'emplacements distincts trouvés pour les utilisateurs
Nombre d'utilisateurs	Score unique	sys_user	Nombre total d'enregistrements utilisateur dans votre instance.
Utilisateurs par pays	Carte	sys_user	Répartition des enregistrements utilisateur par pays.

Séparation de domaine et Classification des données

L'application Séparation de domaine est prise en charge pour Classification des données . Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau de prise en charge : Amélioré

- Inclut tous les aspects des niveaux de prise en charge **Basique** et **Standard** .
- Le processus piloté par les données permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas en affecter une autre.
- Les locataires de l'instance doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) pour eux-mêmes. Cette logique et ces paramètres sont attendus pour un fonctionnement normal de l'application.

Exemple de cas d'utilisation : les locataire-clients d'un environnement partagé doivent être en mesure de modifier la matrice d'impact, d'urgence ou de priorité pour définir la priorité au sein de leur domaine.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Comment fonctionne Séparation de domaine dans Classification des données

Pour Séparation de domaine, l'application utilise la séparation de processus pour la Classification des données table [sys_data_classification]. Pour la table Dictionary-Data Class [m2m_dictionary_dataclass], elle utilise la séparation des données. Pour en savoir plus sur la séparation des données et des processus, consultez Séparation de domaine expliquée.

Information associée

Séparation de domaine pour les fournisseurs de services

Traduction automatique

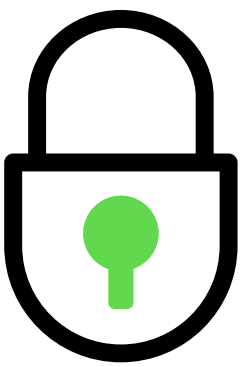
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Chiffrement

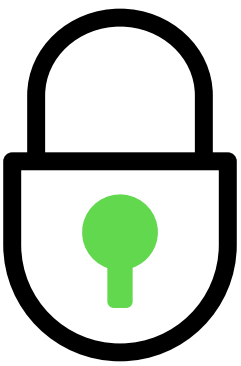
Protégez vos données sensibles et restez conforme aux exigences et normes réglementaires.

Key Management Framework



Utilisez Key Management Framework (KMF) pour personnaliser et gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre instance ServiceNow.

Chiffrement de champ



Utiliser

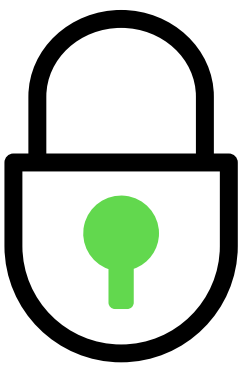
Chiffrement de champ

pour autoriser ou refuser l'accès aux données chiffrées en fonction du rôle de l'utilisateur.

Chiffrement de champ

comprend une gestion de clés de base à l'aide de modules de chiffrement.

Chiffrement de champ Enterprise



Utiliser

Chiffrement de champ

pour autoriser ou refuser l'accès aux données chiffrées en fonction du rôle de l'utilisateur.

Chiffrement de champ

comprend une gestion de clés de base à l'aide de modules de chiffrement.

Chiffrement dans le cloud

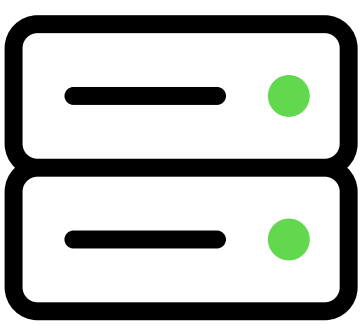


Chiffrez votre base de données d'instance à l'aide du chiffrement de bloc, ainsi que de la gestion améliorée des clés.

Ensemble d'autorisations de chiffrement de plateforme



Chiffrement intégral du disque (FDE)



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

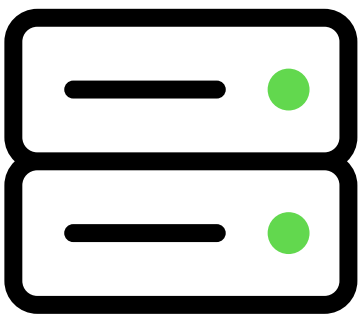
Passer à l’utilisation illimitée

Chiffrement de champ Enterprise

, Chiffrement dans le cloud et Chiffrement de base de données.

Le chiffrement intégral du disque applique le chiffrement à l’ensemble du système de stockage dans le serveur de base de données uniquement. Parce qu’il s’agit du seul composant de stockage des données client.

Chiffrement Edge



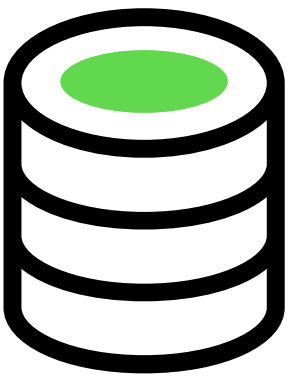
Chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer par Internet à votre instance ServiceNow. Les données restent chiffrées au repos sur l’instance.

Certificats



Utilisez des certificats pour établir des connexions sécurisées et valider les signatures.

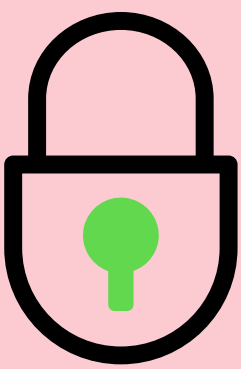
Chiffrement de la base de données



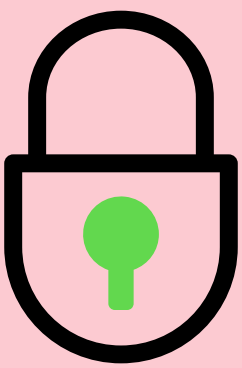
Chiffrez toutes les données stockées en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.

[store-future: BEGIN review]

Key Management Framework



Chiffrement de champ



Chiffrement dans le cloud



Chiffrez votre base de données d’instance à l’aide du chiffrement de bloc, ainsi que de la gestion améliorée des clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez Key Management Framework (KMF) pour personnaliser et gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre instance ServiceNow.

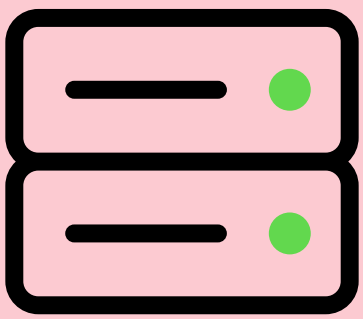
Utilisez Chiffrement de champ pour autoriser ou refuser l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Le chiffrement de champ inclut la gestion de clés de base à l'aide de modules de chiffrement.

Ensemble d'autorisations de chiffrement de plateforme



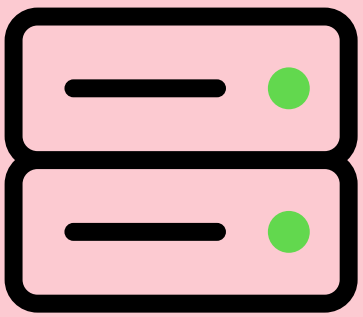
Effectuez une mise à niveau vers Chiffrement de champ Enterprise, Chiffrement dans le cloud et Chiffrement de base de données à usage illimité.

Chiffrement intégral du disque (FDE)



Le chiffrement intégral du disque applique le chiffrement à l'ensemble du système de stockage dans le serveur de base de données uniquement. Parce qu'il s'agit du seul composant de stockage des données client.

Chiffrement Edge



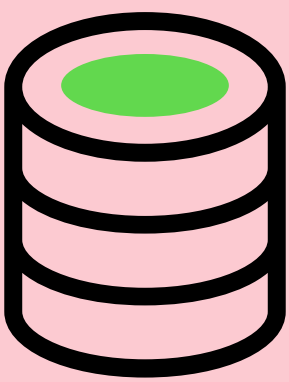
Chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer par Internet à votre instance ServiceNow. Les données restent chiffrées au repos sur l'instance.

Certificats



Utilisez des certificats pour établir des connexions sécurisées et valider les signatures.

Chiffrement de la base de données



Chiffrez toutes les données stockées en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.

Traduction automatique

[End]

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

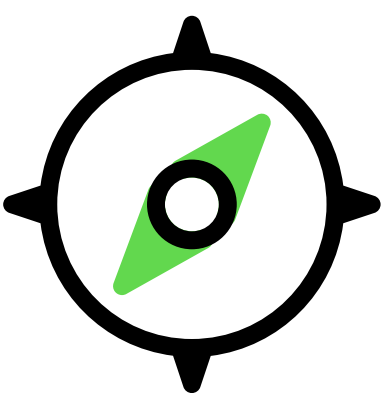
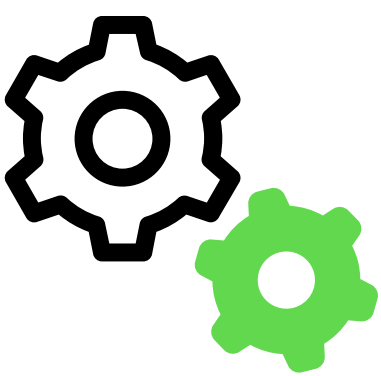
Key Management Framework

Utilisez le Cadre de travail de gestion des clés (KMF) pour générer, échanger, stocker, utiliser et remplacer les clés cryptographiques utilisées pour chiffrer et déchiffrer les données sensibles sur votre ServiceNow instance.

La gestion des clés fait référence aux activités impliquées dans le traitement de vos clés cryptographiques et des paramètres de sécurité associés au cours du cycle de vie de la clé. Cadre de travail de gestion des clés est basé sur les directives 800-57 du National Institute of Standards and Technology (NIST). Conformément à ces directives, vous pouvez utiliser KMF pour :

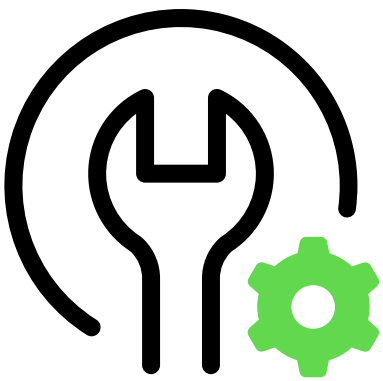
- Affectez des rôles dédiés à la gestion et aux opérations cryptographiques, à l'audit et à l'intégration.
- Créez des modules cryptographiques pour configurer des spécifications cryptographiques à des fins cryptographiques uniques et pour des types de clés uniques.
  - Clé symétrique : chiffrement et déchiffrement, encapsulation et désencapsulation de clés et authentification
  - Clé asymétrique : génération et vérification de signature numérique, chiffrement et déchiffrement, encapsulation et désencapsulation de clé
- Gérer le cycle de vie de votre clé pour générer, faire pivoter, révoquer et suspendre des clés, y compris la prise en charge de plusieurs états clés du cycle de vie
- Créez des politiques d'accès au module (MAP) pour appliquer des contrôles d'accès, pour n'accorder l'accès qu'aux utilisateurs et aux scripts de votre choix.
- Protégez vos clés cryptographiques avec la racine de confiance (RoT) matériel FIPS (Federal Information Processing Standard) 140-2-L3, l'infrastructure à clé publique (PKI), la hiérarchie de clés et le chiffrement d'enveloppe.
- Affectez le rôle d'audit aux utilisateurs afin qu'ils puissent ensuite afficher des informations d'audit telles que les statistiques d'utilisation des clés.

Premiers pas

Explorer le cadre de gestion des clés	Configuration du cadre de travail de gestion des clés	Référence du cadre de travail de gestion des clés
		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrez les composants du cadre de travail de gestion des clés et comment les utiliser pour gérer la façon dont les opérations de chiffrement sont effectuées sur votre instance.	Créez et gérez des composants de gestion des clés pour personnaliser et gérer la façon dont les opérations de chiffrement sont effectuées sur votre ServiceNow ServiceNow.	Créez et gérez des composants de gestion des clés pour personnaliser et gérer la façon dont les opérations de chiffrement sont effectuées sur votre ServiceNow ServiceNow.
	Actions du cadre de travail de gestion des clés  Utilisez les fonctionnalités KMF pour gérer, révoquer ou faire pivoter les clés afin de sécuriser les données sensibles avec les matériaux de chiffrement et les opérations de cycle de vie les plus récents.	

Informations sur l'activation

Le lot d'abonnements ServiceNow à Chiffrement de la plateforme est un droit commercial de groupe qui inclut Cadre de travail de gestion des clés, Chiffrement de champ Enterprise, Chiffrement dans le cloud et Chiffrement de base de données.

Chiffrement de champ Enterprise est la licence illimitée de Chiffrement de champ. Le Chiffrement de champ module d'extension Enterprise est disponible avec l'activation du module d'extension com.glide.now.platform.encryption. Pour plus d'informations, consultez Chiffrement et gestion des clés groupés.

Remarque :
KMF ne prend pas en charge Séparation de domaine, mais peut être utilisé avec les instances sur site.

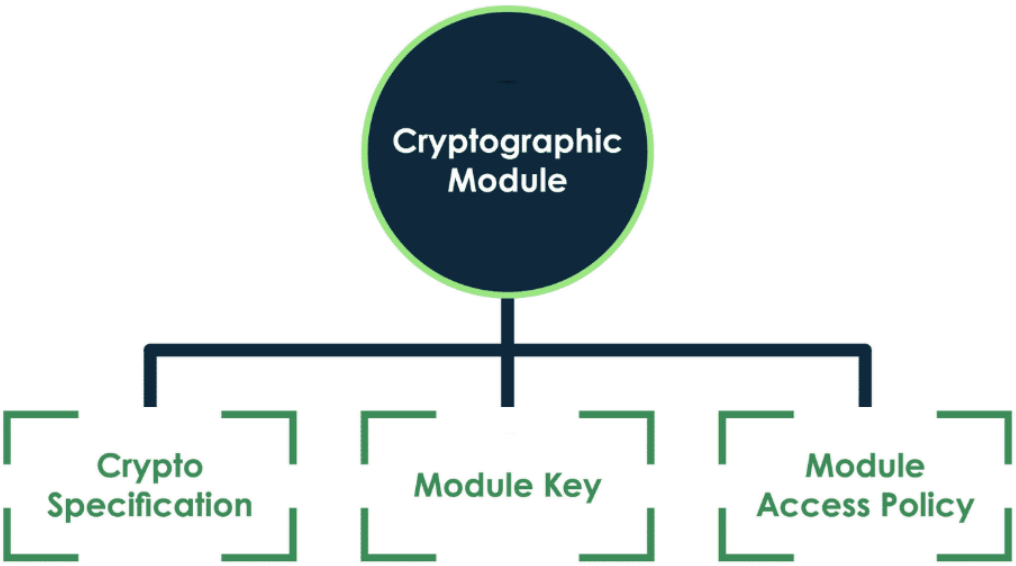
Explorer le cadre de gestion des clés

Découvrez les composants du Cadre de travail de gestion des clés (KMF) et comment les utiliser pour gérer le mode d'exécution des opérations de chiffrement sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composantes du cadre de gestion des clés



Cadre de travail de gestion des clés se compose des composants suivants.

Modules de chiffrement

KMF est centré sur la gestion de modules cryptographiques. Ces modules agissent comme enregistrement parent pour les autres composants. Ils définissent quelles données de votre instance sont chiffrées et quelle méthode de chiffrement utiliser. L'utilisation de plusieurs modules vous permet de chiffrer différentes zones de votre instance avec différentes spécifications.

Par exemple, vous pouvez créer un module pour sécuriser les données de votre application Ressources humaines pour les utilisateurs disposant d'un rôle spécifique. Vous pouvez ensuite créer un autre module pour chiffrer les descriptions d'incident qui sont visibles par certains utilisateurs en fonction d'un script que vous créez.

Les politiques d'accès aux modules sont trouvées en accédant à **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Tous**. Pour en savoir plus sur ces modules, reportez-vous à la section Vue d'ensemble du module de chiffrement.

Clés de module

Les clés cryptographiques sont des chaînes de caractères utilisées en cryptographie. Lorsqu'ils sont utilisés avec un algorithme cryptographique, ils peuvent encoder ou décoder vos données. Ces clés sont utilisées par les spécifications cryptographiques affectées à vos modules. Vous pouvez choisir d'utiliser une clé générée par ServiceNow ou de charger votre propre clé.

Vous pouvez accéder aux clés de module d'un module cryptographique dans la liste connexe **Clés de module** dans les enregistrements de module cryptographique. Pour plus d'informations sur les clés de module, reportez-vous à la section Clés au niveau de l'instance dans le cadre de travail de gestion des clés.

Spécifications cryptographiques

Une spécification cryptographique définit les algorithmes utilisés pour chiffrer vos données. Ces algorithmes utilisent une clé cryptographique pour coder ou décoder vos données. L'affectation d'une spécification cryptographique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

au module détermine la façon dont les données affectées à ce module sont chiffrées.

Vous pouvez accéder aux clés de module d'un module cryptographique dans la liste connexe **Spécifications de chiffrement** dans les enregistrements de module cryptographique. Pour plus d'informations sur les clés de module, reportez-vous à la section Vue d'ensemble des spécifications cryptographiques.

Politiques d'accès au module

Les politiques d'accès aux modules (MAP) sont les contrôles d'accès que vous appliquez à vos modules de chiffrement. Utilisez ces politiques pour déterminer quels utilisateurs et scripts peuvent accéder aux données chiffrées par un module cryptographique.

Recherchez les politiques d'accès aux modules en sélectionnant le lien **Afficher les politiques d'accès** dans les enregistrements du module cryptographique. Pour plus d'informations, consultez Vue d'ensemble de la politique d'accès au module.

Workflow du cadre de travail de gestion de clés

1. **Affecter des rôles KMF**

   Les administrateurs doivent commencer par s'attribuer le rôle sn_kmf.admin. Ce rôle vous permet d'utiliser les fonctionnalités KMF et d'affecter des rôles KMF à d'autres utilisateurs.

2. **Configurer les paramètres KMF**

   Configurez vos paramètres de chiffrement de champ pour sélectionner soit les clés fournies, soit vos propres clés fournies par le client (CSK) pour le chiffrement.

3. **Créer des modules cryptographiques**

   Utilisez des modules cryptographiques pour sélectionner un ensemble de données à chiffrer sur votre instance. Dans les étapes ultérieures, vous affectez une spécification cryptographique pour déterminer comment chiffrer ces données, et une politique d'accès au module pour déterminer qui peut déchiffrer les données.

4. **Créer une spécification cryptographique**

   La spécification cryptographique définit une méthode de chiffrement. Une fois affectées à un module, elles définissent comment les données affectées à ce module sont chiffrées.

5. **Créer des politiques d'accès au module**

   Après avoir créé des modules pour sécuriser vos données, créez des politiques d'accès au module pour contrôler quels utilisateurs et scripts sont en mesure d'accéder aux données chiffrées.

6. **Créer une politique de cycle de vie du module cryptographique**

   Ces stratégies imposent des limites aux modules de chiffrement, telles que la durée de validité d'une clé de chiffrement. Ces politiques peuvent protéger vos modules cryptographiques en limitant leur exposition.

Avantages de Key Management Framework

Avantage	Fonctionnalité	Utilisateurs
Protégez vos données sensibles et propriétaires.	Chiffrement et gestion des clés	Tous
Maintenez la conformité aux directives NIST 800-57. Ces directives sont fournies par le National Institute of Standards and Technology pour	Chiffrement et gestion des clés	Administrateurs de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantage	Fonctionnalité	Utilisateurs
réduire les risques de cybersécurité pour vos réseaux et vos données.		
Utilisez Key Management Framework pour générer, charger, afficher et gérer vos clés cryptographiques. Utilisez la rotation des clés pour une rotation manuelle ou planifiée de vos clés pour une sécurité accrue.	Key Management Framework	Administrateurs de sécurité

Vue d'ensemble du module de chiffrement

Le Cadre de travail de gestion des clés (KMF) est centré sur la gestion des modules cryptographiques. Utilisez ces modules pour sélectionner un mécanisme cryptographique et définir où il est appliqué sur votre instance.

Les modules cryptographiques sont la pièce maîtresse de KMF. Ils définissent les mécanismes cryptographiques spécifiques utilisés pour les opérations cryptographiques pour un cas d'utilisation donné.

Par exemple, vous souhaitez sécuriser les données de votre application Human Resources avec un AES-CBC avec une clé symétrique de 256 bits. Vous pouvez créer un module à cet effet.

Les modules cryptographiques prennent également en charge la gestion du cycle de vie des clés. Vous pouvez créer et faire pivoter vos clés cryptographiques, ainsi que définir votre méthode de chiffrement. Les modules cryptographiques sont composés des composants suivants :

Spécification cryptographique

Définit l'algorithme à utiliser pour le chiffrement et l'origine de la clé. Toutes les clés utilisent la norme de chiffrement avancée avec chaînage de blocs de chiffrement (AES CBC), mais vous pouvez sélectionner 128 ou 256 bits. Cette spécification couvre à la fois les opérations cryptographiques asymétriques et symétriques basées sur les clés.

Remarque :
Le chiffrement symétrique utilise une clé unique pour le chiffrement et le déchiffrement. Le chiffrement asymétrique utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

Clés cryptographiques

Clé que votre module utilise pour coder ou décoder des données cryptographiques. Cette clé peut être générée par votre instance ou une clé fournie par le client que vous créez et chargez.

Politiques d'accès au module

Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès qui limitent le chiffrement ou le déchiffrement des données.

Exceptions de politique du module

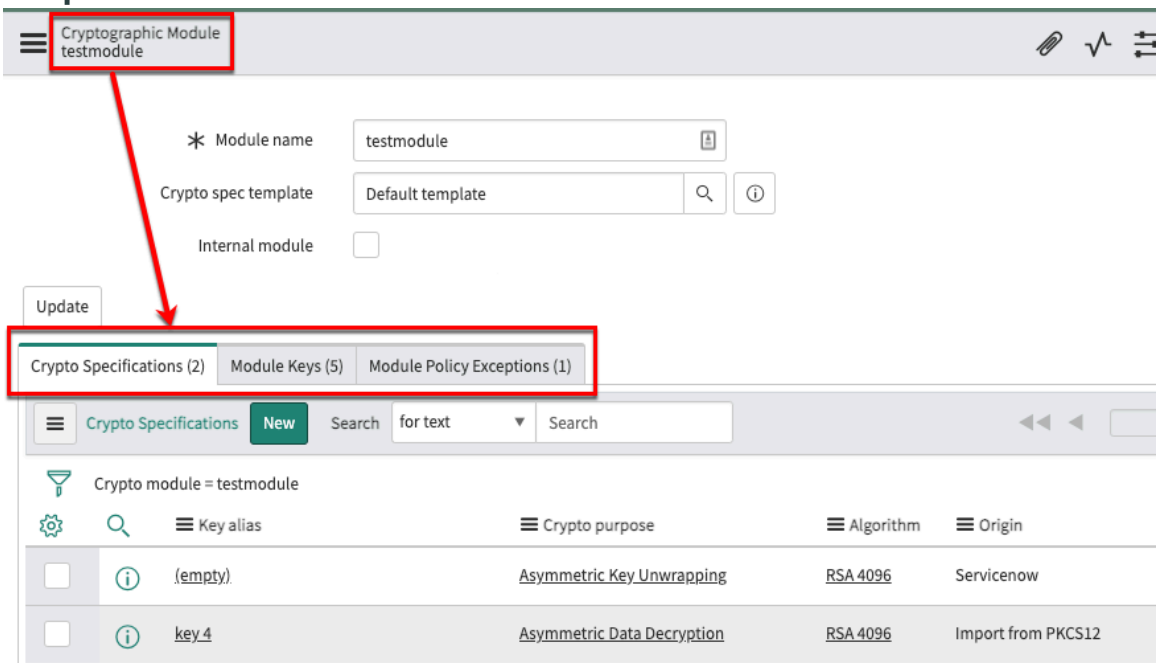
Mécanisme de contrôle pour définir des exceptions à une politique d'accès au module.

L'écran suivant présente ces composants de haut niveau dans un module cryptographique :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants du module de chiffrement



Pour plus d'informations sur la création de modules cryptographiques, reportez-vous à la section Créer un module cryptographique.

Vue d'ensemble des spécifications cryptographiques

La spécification cryptographique est le composant qui définit certains aspects de votre module cryptographique, y compris son objectif cryptographique et l'algorithme de chiffrement à utiliser.

Les spécifications cryptographiques peuvent être adaptées à un objectif cryptographique spécifique, couvrant à la fois les opérations cryptographiques asymétriques et symétriques basées sur des clés. La sélection d'un objectif cryptographique offre d'autres choix, à savoir un ensemble d'algorithmes pris en charge et de configurations de longueur de clé.

Finalités, algorithmes et informations clés de chiffrement

Objectif de chiffrement	Algorithme	Informations clés
Déchiffrement asymétrique des données	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Chiffrement asymétrique des données	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Désencapsulation de clé asymétrique	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Encapsulation de clé asymétrique	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Génération de signature	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Vérification de signature	RSA	Asymétrique : clé 2048 bits, 3072 bits et 4096 bits
Authenticité symétrique	HMAC	Symétrique : clé 256 bits, 384 bits et 512 bits

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Finalités, algorithmes et informations clés de chiffrement (suite)

Objectif de chiffrement	Algorithme	Informations clés
Chiffrement/déchiffrement symétrique des données*	AES-CBC *	Symétrique : clé 128 bits, 192 bits, 256 bits
	AES-BFC	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
Encapsulation/désencapsulation de clé symétrique*	AES-CBC *	Symétrique : clé 128 bits, 192 bits, 256 bits
	AES-BFC	
	AES-OFB	
	AES-CTR	
	AES-GCM **	

* AES-CBC soutient les options de préservation de l'égalité. Chiffrement de champ Enterprise utilise AES-CBC.

** AES-GCM a une intégrité des données intégrée.

La configuration de ces paramètres est abordée dans .Créer un module cryptographique

Vue d'ensemble de la politique d'accès au module

Les politiques d'accès aux modules (MAP) sont des contrôles d'accès que vous appliquez à vos modules de chiffrement. Utilisez ces politiques d'accès pour décider quels utilisateurs et scripts peuvent accéder aux données chiffrées par un module cryptographique.

Politiques d'accès au module

Remarque :
Un abonnement est requis pour utiliser cette Chiffrement de champ Enterprise fonctionnalité. Pour Activer Chiffrement de champ plus d'informations sur Chiffrement de champ Enterprise.

Les politiques d'accès aux modules sont introduites avec le Cadre de travail de gestion des clés (KMF) dans le système de base.

Les politiques d'accès aux modules développent les désignations basées sur les rôles qui ont été fournies avec les modules de chiffrement. Les politiques d'accès aux modules peuvent être basées sur les éléments suivants :

- Basique (périmètre)
- Rôle
- Utilisateur système
- Script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

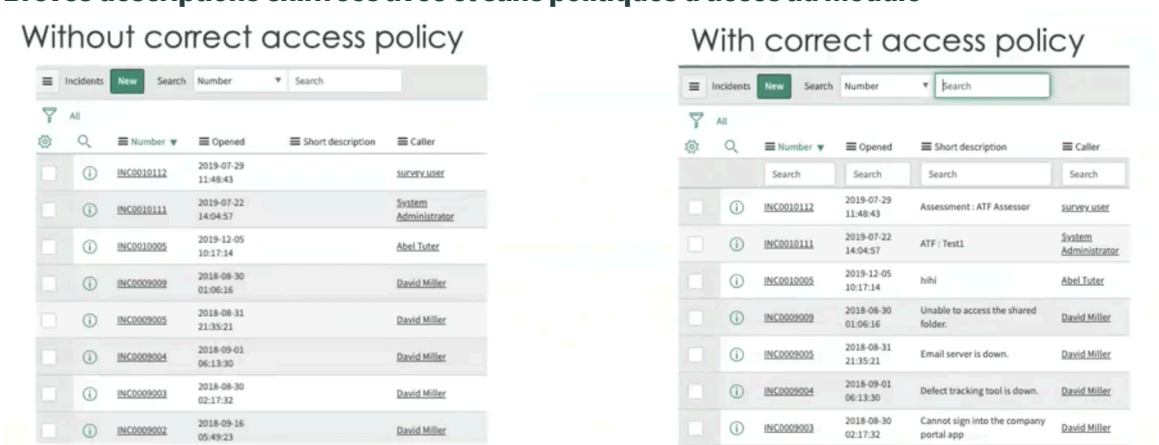
- Resource Exchange

Remarque :
Consultez Échange de ressources du cadre de travail de gestion des clés pour en savoir plus.

Dans un module cryptographique, vous devez configurer les politiques d'accès au module appropriées pour autoriser l'accès aux données chiffrées. Sans politique d'accès au module associée à un module cryptographique, les données chiffrées ne sont pas visibles par les utilisateurs et les champs et colonnes associés dans les listes s'affichent vides.

Dans cet exemple, l'absence d'une politique d'accès au module sur le champ Brève description chiffrée masque le contenu à tous les utilisateurs accédant à la table Incident. Avec une politique d'accès au module en place, seuls les utilisateurs ayant un rôle spécifique peuvent voir les données chiffrées.

Brèves descriptions chiffrées avec et sans politiques d'accès au module



Remarque :
Les données de la colonne apparaissent également vides pour les utilisateurs dont le rôle approprié n'est pas spécifié dans la politique d'accès au module.

Reportez-vous à pour Créer une politique d'accès au module la configuration.

Politiques de génération automatique

Les politiques de génération automatique sont automatiquement générées par le système en fonction de la politique d'accès au module par défaut définie pour le module de chiffrement donné. Si aucune politique de niveau granulaire n'est définie lorsque le système ou un script tente d'accéder au module de chiffrement donné, ces politiques globales sont générées et appliquées.

Important :

Les règles de politique de génération automatique ne sont pas appliquées aux types de travaux planifiés ou aux modules de chiffrement de champ (modules où se trouve Chiffrement de champ le module parent).

Clés au niveau de l'instance dans le cadre de travail de gestion des clés

Découvrez la structure de clé (KMF), qui utilise le Cadre de travail de gestion des clés chiffrement d'enveloppe pour garantir que toutes les clés de plateforme gérées KMF sont protégées par une chaîne de clés. Les clés de chiffrement des données client (CDEK) créées par KMF sont également incluses dans cette structure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

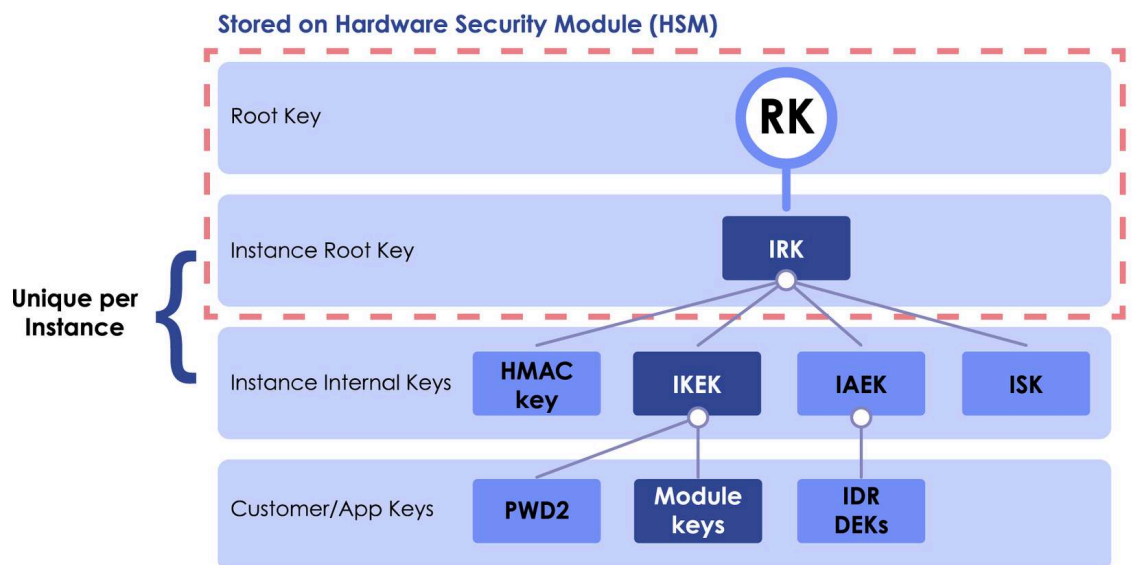
.

Architecture de stockage de clés KMF

La KMF structure de clés utilise le module de sécurité matériel (HSM) SafeNet KeySecure. Le HSM est conçu pour être physiquement et électroniquement inviolable afin de répondre à la norme de sécurité FIPS 140-2-L3 . KMF utilise le chiffrement d'enveloppe pour s'assurer que toutes les clés de plateforme sous KMF gestion sont protégées par une chaîne de clés, y compris les clés de module qui peuvent être générées par KMF.

Chiffrement de l'enveloppe

Le chiffrement d'enveloppe est la pratique consistant à chiffrer une clé avec une autre clé, également appelée enveloppement. Les clés de module sont chiffrées par la clé de chiffrement de clé d'instance (IKEK), qui à son tour est chiffrée par la clé racine d'instance (IRK), qui est enfin chiffrée par la clé racine (RK). Étant donné que l'IRK n'est accessible que par le HSM, l'IKEK doit être téléchargé pour le déchiffrement.



Au niveau de l'instance, KMF définit plusieurs clés qui sont utilisées en interne à des fins cryptographiques diverses dans l'ensemble de la ServiceNow AI Platform.

Ce tableau fournit des exemples d'un sous-ensemble de clés disponibles qui sont gérées et protégées par KMF.

Clé	Emplacement	Description
Clé racine (RK)	Modèle de sécurité matérielle (HSM)	Clé racine utilisée pour déchiffrer l'IRK.
Clé racine d'instance (IRK)	HSM	Une clé unique à votre instance qui est utilisée pour chiffrer dans une enveloppe plusieurs clés internes d'instance.
Clé HMAC d'instance (IHK)	Instance	Unique par instance, l'IHK est utilisé en interne à des fins de code d'authentification de message basé sur le hachage (HMAC).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clé	Emplacement	Description
		La IHK permet de vérifier l'authenticité et l'intégrité des clés de module et est encapsulée dans KeySecure ou dans le magasin de clés de fichier.
Clé de chiffrement de clé d'instance (IKEK)	Instance	L'IKEK encapsule les clés du module et est encapsulé dans KeySecure ou dans le magasin de clés de fichier.
Clé de chiffrement asymétrique d'instance (IAEK)	Instance	Clé unique à votre instance qui est utilisée en interne à des fins de chiffrement asymétrique. L'IAEK est utilisé pour transmettre des messages confidentiels entre une instance pendant ou Réplication de données d'instance l'approbation Key Exchange du consommateur.
Clé de signature d'instance (ISK)	Instance	Une clé unique à votre instance qui est utilisée en interne à des fins de signature.
Password2 (PW2)	Instance	Avec KMF, la clé pour PW2 les champs est entièrement gérée par KMF.
Clé de chiffrement des données client (CDEK)	Instance	Les clés de chiffrement créées par l'intermédiaire KMF sont cryptées par enveloppe par l'IKEK.
Réplication de données d'instance (IDR) Clé de chiffrement des données (DEK)	Instance	Clés de chiffrement spécifiques utilisées pour le processus IDR.

Configuration du cadre de travail de gestion des clés

Créez et gérez des composants de gestion des clés pour personnaliser et gérer la façon dont les opérations de chiffrement sont exécutées sur votre ServiceNow instance.

Affecter des Cadre de travail de gestion des clés rôles

Les administrateurs disposant du rôle security_admin peuvent affecter Cadre de travail de gestion des clésKMF() des administrateurs, qui à leur tour peuvent affecter d'autres Cadre de travail de gestion des clés rôles.

Avant de commencer
Rôle requis : admin et security_admin

Vous devez accéder au rôle security_admin avant d'affecter le KMF rôle administrateur. Pour obtenir des instructions, consultez Accéder à un rôle privilégié.

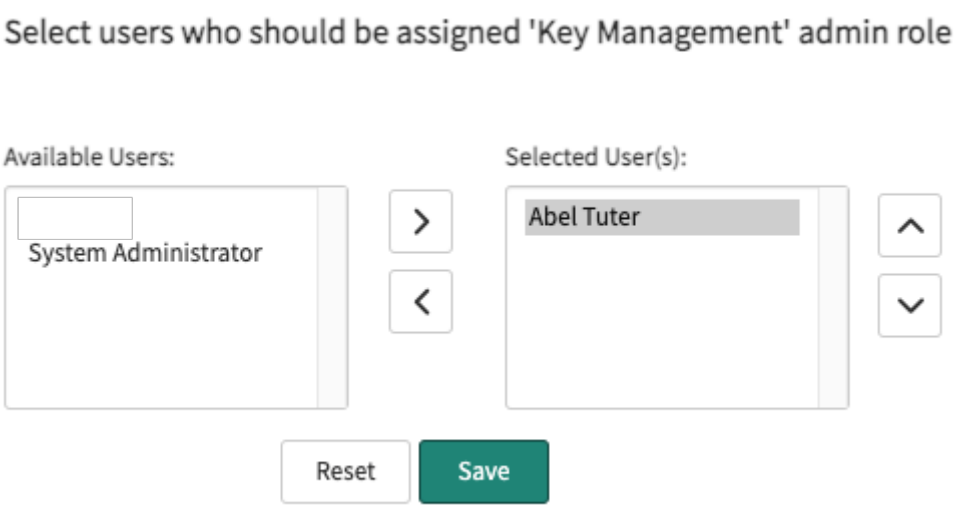
Important :
KMF rôles sont requis pour utiliser le Cadre de travail de gestion des clés. Les utilisateurs sans KMF rôles ne peuvent pas accéder aux listes, tables et modules utilisés pour configurer la gestion des clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accéder au rôle d'administrateur de sécurité.
2. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur dont vous souhaitez être l'administrateur KMF .
3. Si l'utilisateur ne dispose pas déjà des rôles administrateur et security_admin, sélectionnez **Modifier** sous la liste connexe Rôles et ajoutez des _admin **administrateur** et **de sécurité**.
4. Accédez à la **Sécurité de système** > **Administration de la gestion de clés**.
5. Sélectionnez l'utilisateur que vous souhaitez définir comme KMF administrateur dans la colonne **Utilisateurs disponibles** et déplacez-le vers la colonne **Utilisateurs sélectionnés** .

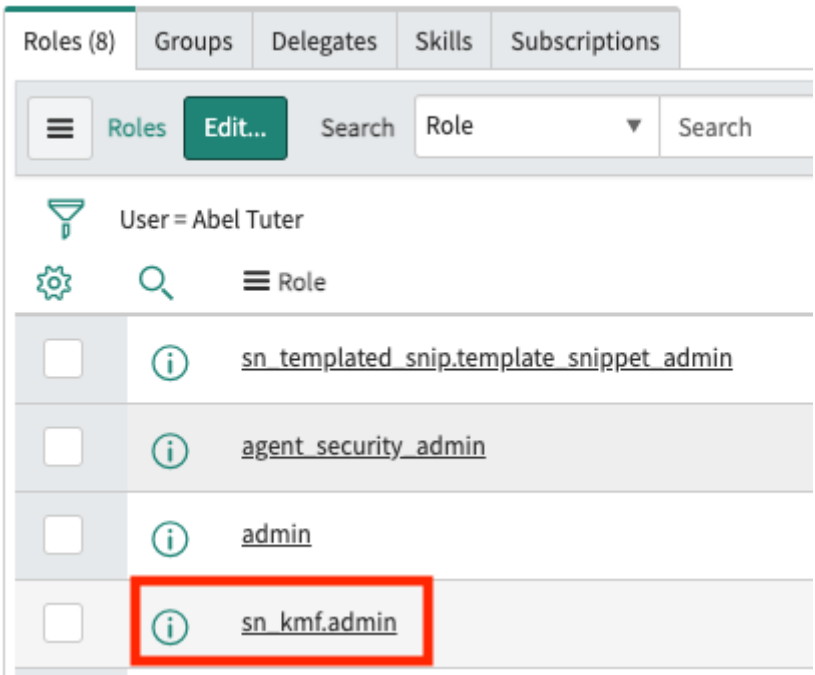


6. Sélectionnez **Enregistrer**.
7. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur à qui vous venez de donner le rôle administrateur KMF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

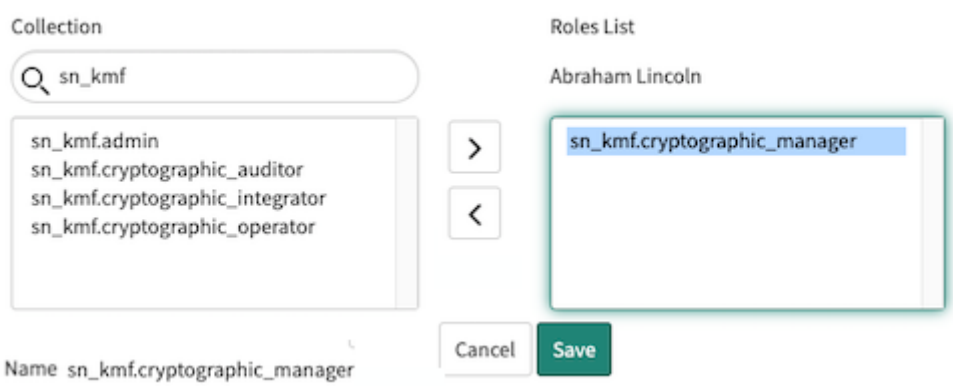
Cet utilisateur dispose désormais du rôle sn_kmf.admin dans la liste connexe Rôles. Cet utilisateur peut désormais affecter d'autres rôles KMF.



Que faire ensuite

Si vous disposez du rôle administrateur KMF, procédez comme suit pour affecter d'autres rôles KMF :

1. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur auquel vous souhaitez attribuer un autre rôle KMF, tel que Gestionnaire de chiffrement KMF.
2. Dans la liste connexe Rôles, cliquez sur **Modifier** et sélectionnez les rôles KMF que vous souhaitez affecter aux utilisateurs. Tous les rôles KMF commencent par sn_kmf.



Que faire ensuite

Pour en savoir plus sur les rôles disponibles KMF , reportez-vous à la section Rôles installés avec Key Management Framework.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé

Configurez vos paramètres de chiffrement de champ pour utiliser ServiceNow les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur le ServiceNow AI Platform.

Avant de commencer

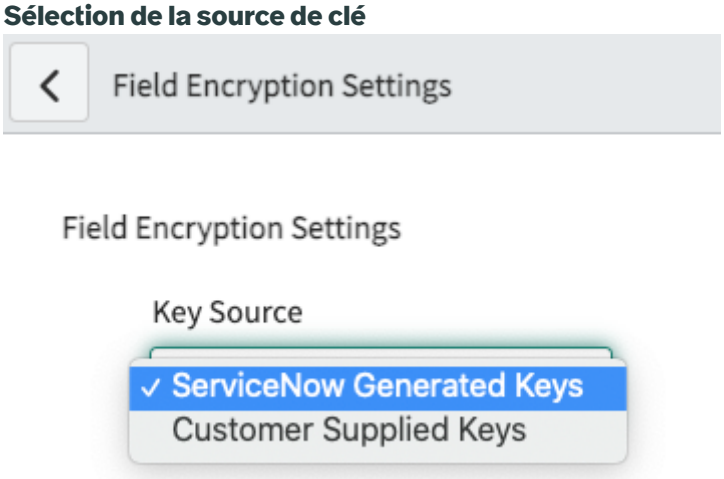
Les clés fournies par le client ne sont prises en charge qu'avec Chiffrement de champ Enterprise.

Rôle requis : sn_kmf.cryptographic_manager et security_admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Paramètres de Chiffrement de champ**.
2. Dans les paramètres de chiffrement de champ, sélectionnez **Clés générées par ServiceNow** ou **Clés fournies par le client** dans la liste **Source de clés** .

Sélection de la source de clé



Cette option remplace la propriété `com.glide.encryption.cle_kmf.key_source` par **Clés générées par ServiceNow** ou **Clés fournies par le client**.

3. Sélectionnez **Enregistrer**.

Que faire ensuite

- Si vous utilisez vos propres clés fournies par le client, reportez-vous à la section Utilisation des clés fournies par le client avec Chiffrement de champ Enterprise.
- Si vous utilisez ServiceNow les clés fournies, commencez à créer votre module cryptographique. Consultez Créer un module cryptographique.

Créer un module cryptographique

Créez un module cryptographique pour définir les mécanismes utilisés pour les opérations cryptographiques. Après avoir créé le module, vous créez une spécification cryptographique, dans laquelle vous définissez un algorithme de chiffrement et générez une clé.

Avant de commencer

Si vous fournissez vos propres clés, rendez-vous sur Configurer et charger la clé fournie par le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles KMF dans le système de base de la ServiceNow plateforme. Chiffrement de champ Enterprise La fonctionnalité n'est disponible que lorsque le module `d'extension com.glide.now.platform.encryption` est actif. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de . Consultez Créer un module cryptographique pour Chiffrement de champ.

Remarque :
Les enregistrements du module de chiffrement [sys_kmf_crypto_module] ne peuvent pas être supprimés.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Créer**.
2. Renseignez les champs suivants du formulaire :

Champs du module de chiffrement

Champ	Description
Nom du module	Chaîne alphanumérique à référencer lors de l'exécution de scripts.
Modèle de spécification de chiffrement	Sélectionnez le modèle **par défaut** à utiliser pour créer le module de chiffrement, car il contient des mappages des algorithmes pris en charge pour les spécifications cryptographiques.
Valeur de la politique d'accès au module par défaut	○ S'appuyer sur le système par défaut : ○ Refuser ○ Trace
Résultat réel de la politique d'accès au module	Rejeter ou suivre, en fonction de la valeur de politique par défaut ou de la valeur sélectionnée lors de la création de la politique d'accès au module.
Nom	Nom du module de chiffrement précédé du nom du périmètre de l'application.
État du cycle de vie du module de chiffrement	Le cycle de vie fait référence à la création, l'utilisation et la désactivation d'un module cryptographique. Définir sur **Brouillon** initialement pendant la configuration. Lorsque vous utilisez le module, définissez ce champ sur **Publié**. Le modèle par défaut est automatiquement défini sur Publié.

3. Sélectionnez **Soumettre**.

Avertissement :

Pour les utilisateurs de la prise en charge du chiffrement hérité :

Si vous utilisez la version non entreprise de Chiffrement de champ, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre maximal de modules publiés autorisés Chiffrement de champ avec le produit d'abonnement. L'abonnement Entreprise pour Chiffrement de champ est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l'envoi réussi, votre module de chiffrement est répertorié dans la table Modules de chiffrement. Le système ajoute le nom au champ d'application pour éviter tout conflit avec d'autres applications incluses dans le périmètre. Par exemple, si vous avez créé un module portant le nom `my_crypto_module` dans le périmètre de l'application global, le nom est enregistré en tant que `global.my_crypto_module`.

Que faire ensuite

Créer une spécification cryptographique

.

Créer une spécification cryptographique

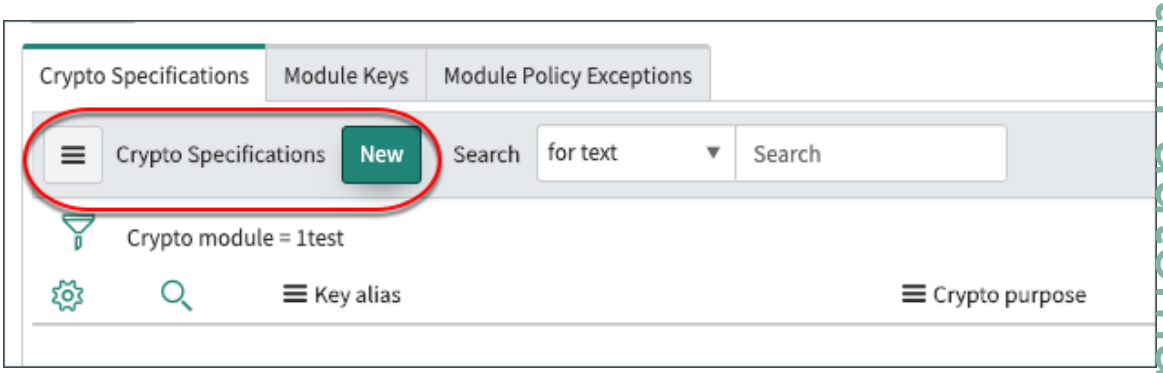
Après avoir créé un module cryptographique, créez une spécification cryptographique pour définir les algorithmes du module.

Avant de commencer

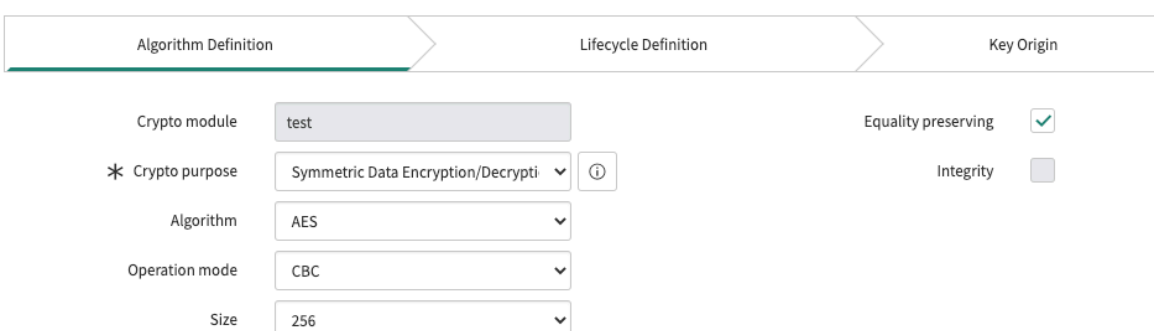
Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module cryptographique pour la définition afin d'ouvrir les options de configuration.
3. Dans l'onglet **Spécifications cryptographiques** , sélectionnez **Nouveau**.



4. Remplissez le formulaire Définition de l'algorithme.
   Consultez Vue d'ensemble des spécifications cryptographiques pour en savoir plus.



L'écran de définition de l'algorithme s'ouvre. Sélectionnez les options pour la génération de clés. Répétez cette étape pour générer plusieurs clés pour le module de chiffrement sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de définition de l'algorithme

Champ	
Module de chiffrement	Lecture seule. Le nom du module de chiffrement sélectionné s'affiche.
Objectif de chiffrement	Sélectionnez l'objectif de ce module. Par exemple, vous pouvez l'utiliser pour le chiffrement de données, la génération de signatures ou l'emballage de clés. Les algorithmes disponibles s'ajustent en fonction de l'objectif de chiffrement sélectionné. Consultez Vue d'ensemble des spécifications cryptographiques pour en savoir plus.
Algorithme	Type d'algorithme utilisé pour atteindre l'objectif de crypto. L'algorithme contrôle également l'origine de la clé. S'ajuste automatiquement en fonction de l'objectif de chiffrement sélectionné. Vue d'ensemble des spécifications cryptographiques pour en savoir plus.
Mode d'opération	Ce champ peut s'afficher en fonction de l'objectif de chiffrement sélectionné.
Taille	Sélectionnez la taille du bit.
Hachage	Ce champ devient disponible en fonction de l'algorithme sélectionné.
Préservation de l'égalité	Active le chiffrement non déterministe. Cette option s'affiche lorsque vous sélectionnez **Chiffrement/déchiffrement de données symétriques** avec **AES** et en mode **CBC (Cipher Block Chaining**). La sélection de cette option signifie que si les mêmes données sont à nouveau chiffrées, les données codées sont les mêmes à chaque fois. Le chiffrement non déterministe ne prend pas en charge le filtrage d'une liste de données chiffrées à l'aide d'opérateurs de comparaison d'égalité.
Intégrité	Le mode de fonctionnement GCM assure l'intégrité.

5. Sélectionnez **Suivant**.
   La spécification de chiffrement est répertoriée dans la table Cycle de vie de la clé en fonction des algorithmes sélectionnés.

Que faire ensuite

Effectuez l'une des opérations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Pour plus d'informations, consultez Configurer les états clés du cycle de vie la rubrique pour compléter la définition du cycle de vie de la clé.
- Sélectionnez **Suivant** pour créer une clé cryptographique. Consultez l'une des tâches suivantes pour la génération de clés :
  - Générer une clé cryptographique ServiceNow.
  - Configurer les propriétés des clés fournies par le client.
  - Importer la paire de clés d'encapsulation/de désencapsulation.

Configurer les états clés du cycle de vie

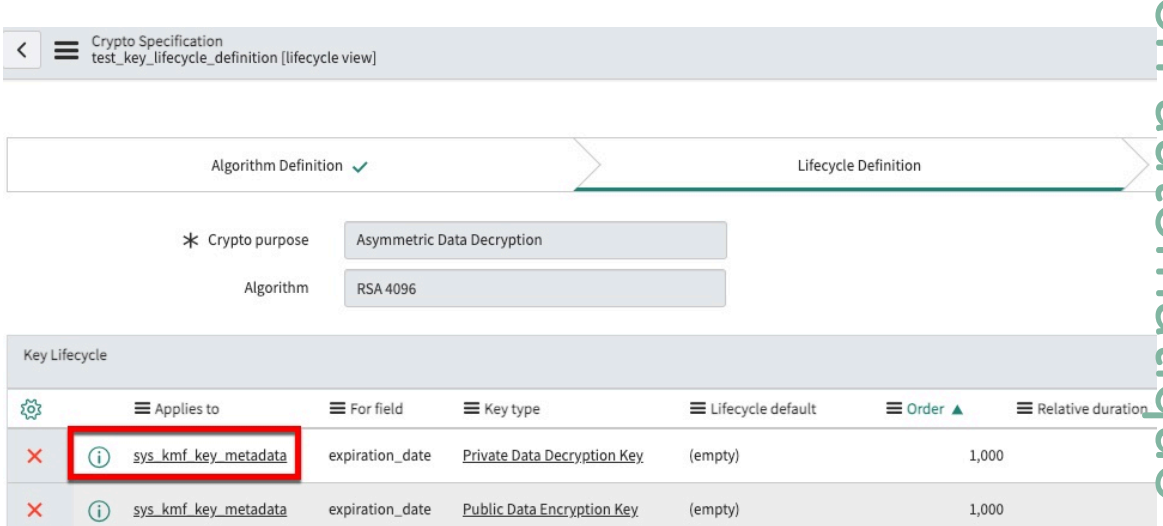
Une fois que vous avez créé une spécification cryptographique, vous pouvez configurer les actions de cycle de vie des clés de votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin

Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module de chiffrement pour configurer le cycle de vie d'une clé.
3. Sélectionnez un alias de clé dans l'onglet Spécifications de chiffrement.



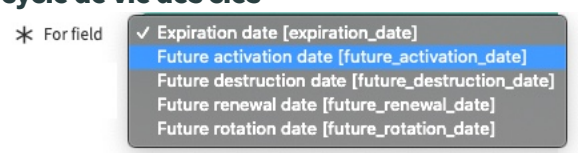
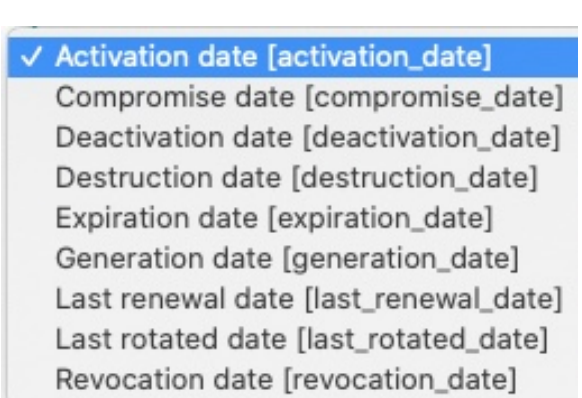
4. Sélectionnez **Suivant**.
   Le modèle de cycle de vie du champ se charge. Les valeurs du cycle de vie de la clé par défaut sont créées en fonction des algorithmes sélectionnés pour la spécification cryptographique définie.
5. Sélectionnez un cycle de vie de clé dans la colonne **S'applique à** de l'étape Définition du cycle de vie pour la spécification de chiffrement.

Champs du cycle de vie de la clé

Champ	Description
Concerne	Clé sélectionnée à laquelle le cycle de vie s'applique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Pour le champ	Sélectionnez le type de contrôle pour la clé à laquelle le cycle de vie s'applique. **Valeurs « Pour le champ » de la gestion du cycle de vie des clés** 
Type	Sélectionnez si l'évaluation pour le cycle de vie de clé est une valeur relative ou une valeur absolue : ○ **Relative** : entrez une valeur qui dépend d'autres entrées de données dans le système, telles que la génération, l'activation et la désactivation de clés. ○ **Absolu** : saisissez une valeur exacte, telle qu'une date.
Valeur par défaut du cycle de vie	Lecture seule. Affiche une valeur si définie.
Ordre	Entrez la séquence dans laquelle traiter l'état du cycle de vie de la clé pour la spécification crypto.
Type de durée relative	Durée du cycle de vie : **années**, **mois** ou **jours**.
Durée relative	Nombre d'années, de mois ou de jours pendant lesquels la clé est valide.
Opération relative	**avant**ou **après**.
Relatif à	Champ auquel la durée est relative. S'affiche si une durée ou une opération relative est sélectionnée. 

Traduction automatique

Générer une clé cryptographique ServiceNow

Suivez cette procédure pour charger et configurer une clé cryptographique afin de chiffrer des ServiceNow données sensibles.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

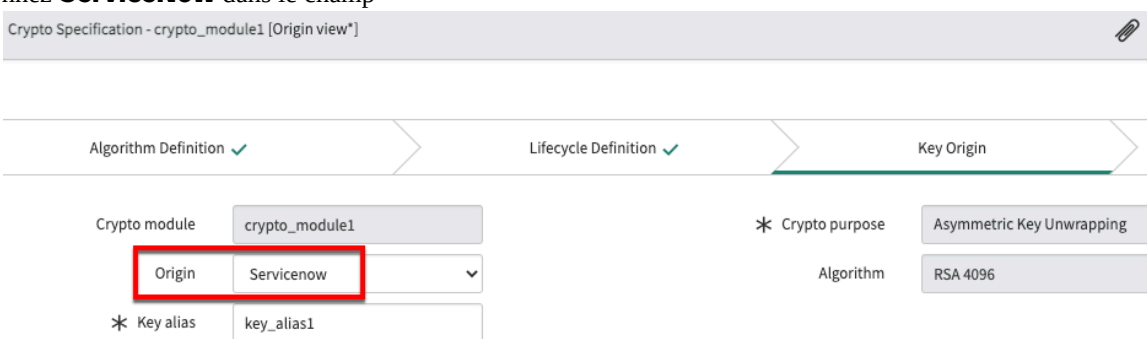
Pourquoi et quand exécuter cette tâche
Les gestionnaires cryptographiques ont le choix d'utiliser ServiceNow les clés fournies ou leurs propres clés fournies par le client (CSK) pour le chiffrement sur le ServiceNow AI

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Platform .Chiffrement de champ Enterprise Pour en savoir plus sur CSK, reportez-vous à la section Configurer les propriétés des clés fournies par le client.

Procédure

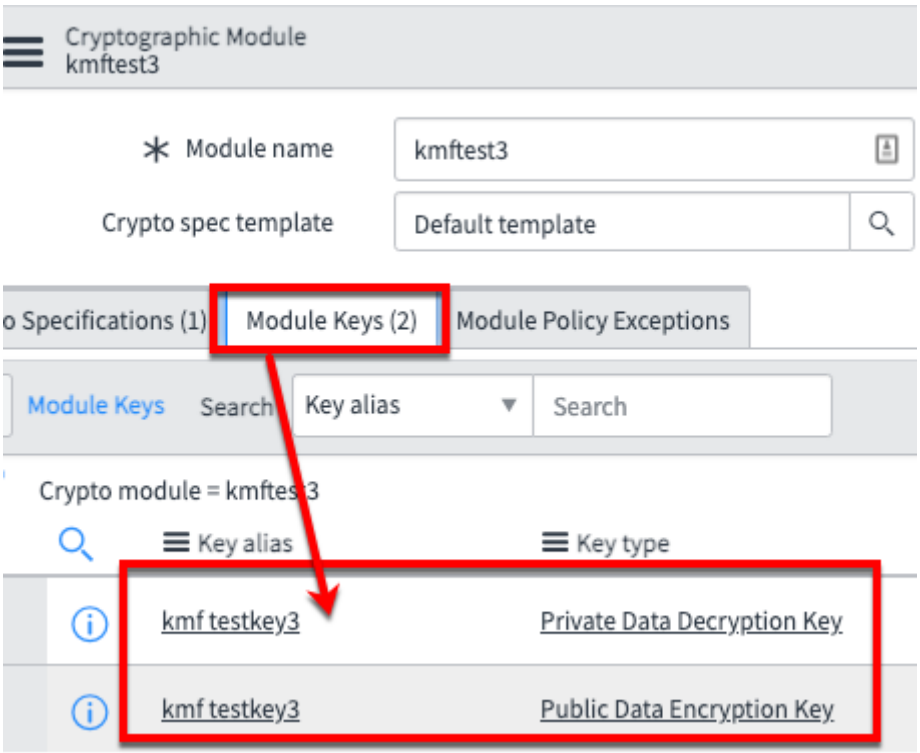
1. Définissez les paramètres de chiffrement de champ pour utiliser les clés générées par ServiceNow.
   Consultez Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé pour en savoir plus.
2. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
3. Sélectionnez le module cryptographique correspondant pour ouvrir la page des détails du module cryptographique.
4. Sélectionnez la ligne pour l'entrée d'alias de clé dans l'onglet Spécifications cryptographiques.
   Si aucune clé n'a encore été générée, le champ Alias de la clé est vide.
5. Sélectionnez **Suivant** pour accéder à l'onglet Origine de la clé des composants de spécification crypto.
   L'onglet Définition du cycle de vie s'affiche avec la table du cycle de vie de la clé et peut être examiné ou modifié. Consultez Configurer les états clés du cycle de vie pour en savoir plus.
6. Sélectionnez **ServiceNow** dans le champ



   Origine.
   Ce champ varie en fonction des paramètres de chiffrement de champ de l'étape 1 et de l'algorithme sélectionné. Pour utiliser une clé importée, reportez-vous à la section Importer la paire de clés d'encapsulation/de désencapsulation. Voyez Configurer les propriétés des clés fournies par le client si vous utilisez votre propre clé.
7. Saisissez un nom convivial pour l'alias de clé.
8. Sélectionnez **Suivant** pour passer à l'onglet Création de clé.
9. **Sélectionnez Générer la clé**.
   Une fois la clé générée, le formulaire Module cryptographique se recharge et affiche à nouveau la spécification cryptographique.
10. Sélectionnez l'onglet **Clés de module** pour afficher les clés.
    Les informations sécurisées de la clé sont stockées dans l'onglet Clés de module, ainsi que le nombre de clés qui existent pour la spécification cryptographique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Sélectionnez une clé pour effectuer des actions de gestion des clés.
Consultez Actions de gestion des clés pour en savoir plus.

Créer une politique d'accès au module

Créez des politiques d'accès au module pour déterminer quels utilisateurs et scripts peuvent accéder aux données chiffrées par un module cryptographique.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Chiffrement de champ prend en charge les politiques d'accès au module basées sur les rôles et des options de configuration supplémentaires deviennent disponibles avec la fonctionnalité (CLE_Ent).

- Configurez l'opération de chiffrement spécifique dans les stratégies d'accès au module pour les modules de chiffrement qui prennent en charge les opérations symétriques. Par exemple, un utilisateur peut être autorisé à chiffrer des données mais pas à déchiffrer des données.
- Définissez une valeur de politique d'accès au module par défaut ou en fonction d'un module cryptographique.
- Associez les versions de script où les changements apportés au script sont suivis et invalidez la politique de script, offrant ainsi une meilleure sécurité pour les politiques d'accès au module de type script.

CLE_Ent est disponible avec un abonnement payant. Consultez la rubrique pour connaître les fonctionnalités prises en charge et les options disponibles avec chaque offre. Pour plus d'informations, consultez Chiffrement de champ Enterprise.

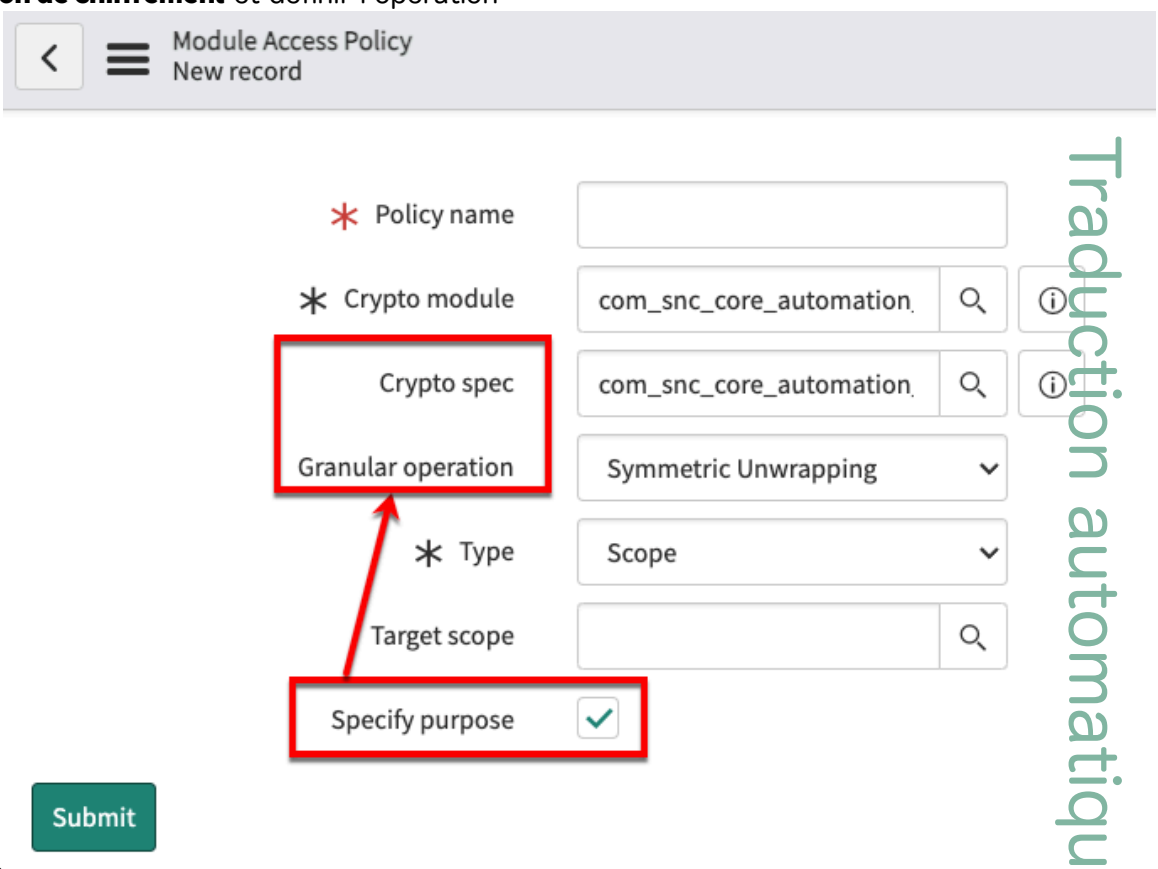
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le comportement par défaut des politiques d'accès au module (MAP) est Rejeter pour empêcher tout accès non autorisé, sauf déclaration explicite dans les enregistrements MAP.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
   Si vous ne créez pas de module de chiffrement configuré pour le chiffrement/déchiffrement de données symétriques, une politique d'accès au module générée automatiquement est créée et répertoriée dans la table.
2. Sélectionnez **Nouveau**.
   - Sélectionnez **Spécifier l'objectif** pour choisir une **spécification de chiffrement** et définir l'opération **granulaire**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Avec les spécifications cryptographiques pour le chiffrement/déchiffrement de données symétriques et l'encapsulation/désencapsulation symétrique, le champ **Opération granulaire** est disponible si vous cochez la case **Spécifier l'objectif** .



3. Renseignez le formulaire.

Champs de politiques d'accès au module

Champ	Description
Nom de la politique	Saisissez un nom pour la politique.
Module de chiffrement	Sélectionnez l'icône de recherche (icône pour sélectionner un module.
Spécification du chiffrement	Sélectionnez ou créez une spécification cryptographique lors de la génération de la politique d'accès au module. Ce champ est disponible lorsque la case **Spécifier l'objectif** est cochée.
Opération granulaire	Sélectionnez l'objectif cryptographique de la spécification cryptographique. Les valeurs disponibles dépendent du type de spécification cryptographique sélectionné. Voir pour plus de détails sur les objectifs cryptographiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	○ **Périmètre** : contrôle l'accès par périmètre de l'application. ○ **Utilisateur système** : autorise les utilisateurs système à accéder aux modules de chiffrement. ○ **Script** : contrôler l'accès par script. Pour plus d'informations, consultez ○ **Rôle** : contrôle l'accès par rôle d'utilisateur. ○ **Échange de ressources** : contrôlez l'accès à l'aide du Resource Exchange fichier . Consultez pour plus d'informations. **Remarque :** Seul le type de rôle est pris en charge avec Chiffrement de champ. Tous les autres types sont disponibles avec Chiffrement de champ Enterprise.
Périmètre cible	Le champ est visible en tant qu'identificateur pour le type **de champ d'application** . Fait référence à la fonctionnalité de la politique. Sélectionnez les applications dans le menu de recherche. **Remarque :** Le champ d'application cible n'est pas pris en charge et ne peut être défini qu'avec Chiffrement de champ Enterprise
Rôle cible	Le champ est visible en tant qu'identificateur pour le type **de rôle** . Rôle auquel cette politique s'applique.
Table de scripts Script cible	Ces champs s'affichent lorsque vous sélectionnez **Script** comme type. Le champ est visible en tant qu'identificateur pour le type **de script** . Sélectionnez une table à laquelle cette politique s'applique. Document auquel cette politique s'applique. Sélectionnez le **nom** de la table, puis le document connexe pour la politique. La première fois qu'un script appelle un module cryptographique, l'accès au module est refusé et le développeur reçoit une erreur. Cette erreur donne au propriétaire du module la possibilité d'accorder ou de refuser l'accès au module.
Échange de ressources : ○ Spécification du chiffrement ○ Type d'approbation ○ Hôte de l'instance cible	Ces options s'affichent lorsque vous sélectionnez le type. Resource Exchange est pris en charge à la fois par KMF et par lorsque le module parent est **column_level_encryption**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Sélectionnez la spécification de chiffrement, Unique ou Récurrent, et l'URL de l'instance cible. Consultez pour plus d'informations.
Emprunt d'identité	Dans les stratégies d'accès au module basées sur les rôles, les utilisateurs peuvent accéder aux données chiffrées à l'aide d'une session d'emprunt d'identité. Lorsque des utilisateurs, tels que des administrateurs, empruntent l'identité d'autres utilisateurs, ces politiques d'accès au module activées pour l'emprunt d'identité sont appliquées.
Spécifier l'objectif	Sélectionnez cette option pour que le champ Spécification cryptographique soit disponible pour la politique.
Actif	Sélectionnez cette option pour activer la politique.
Résultat	Sélectionnez l'une des options suivantes : ○ **StrictReject** rejette l'accès en toutes circonstances. ○ **Rejeter** empêche les utilisateurs ayant le **rôle cible** ou le **champ d'application cible** d'accéder à ce module de chiffrement, sauf si une autre politique leur accorde l'accès. ○ **Suivi** permettant d'autoriser l'accès au module et de surveiller son utilisation.

4. Sélectionnez **Soumettre**.

Avertissement :

Pour les utilisateurs de la prise en charge du chiffrement hérité :

Si vous utilisez la version non entreprise de Chiffrement de champ, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de modules publiés autorisés Chiffrement de champ avec le produit d'abonnement. L'abonnement Entreprise pour Chiffrement de champ est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

5. Sélectionnez le nom de politique associé au module de chiffrement que vous souhaitez examiner.
Utilisation de la politique d'accès au module de type de script :

Une politique d'accès au module est générée automatiquement en fonction du paramètre d'accès par défaut lors de l'exécution du script. Le nom du module est précédé de AutoGen-. Par exemple, le module Module-TestPolicy est répertorié sous le nom AutoGen-Module-TestPolicy dans la colonne Nom de la politique.

Le formulaire Politique d'appelant cryptographique répertorie la politique d'appelant que vous avez sélectionnée. Le champ Périmètre cible spécifie le périmètre du script qui tente d'utiliser le module. Consultez la section pour plus d'informations.

Remarque :
Un maximum de cinq politiques d'accès au module est autorisé avec Chiffrement de champ. Consultez la section pour les options de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une politique d'accès au module de rôle granulaire pour le chiffrement symétrique

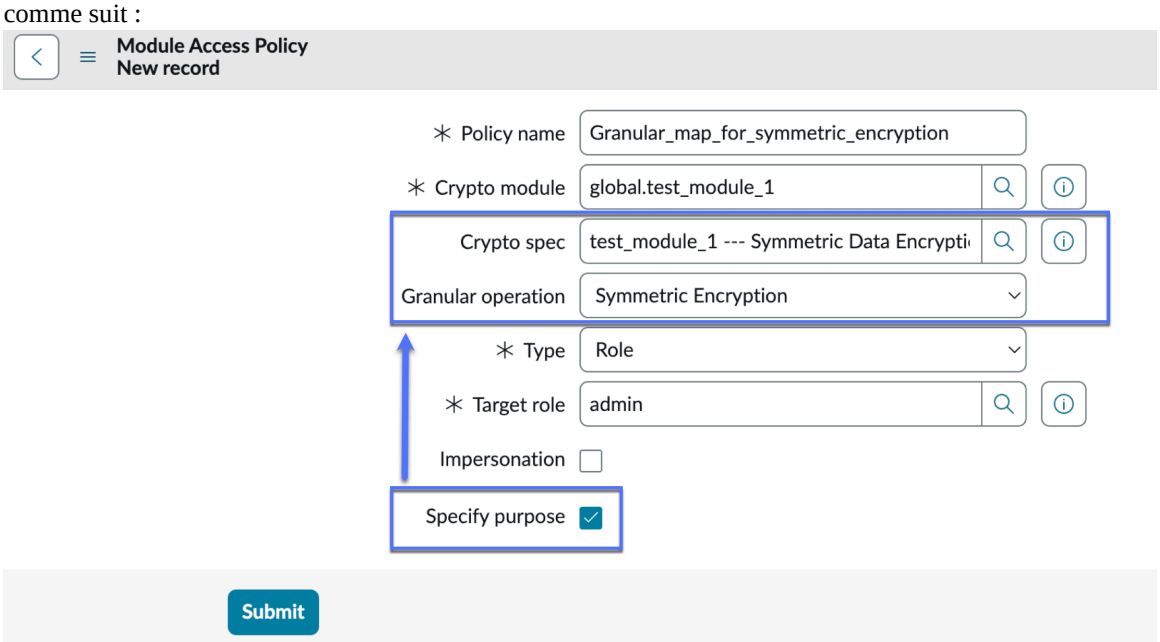
Créez une politique d'accès au module de rôle granulaire (MAP) pour sécuriser les données tout en permettant aux utilisateurs non affectés à une MAP spécifique de soumettre des formulaires sur un enregistrement public.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
2. Sélectionnez **Nouveau**.
3. Saisissez un nom pour la politique.
4. Sélectionnez le **module de chiffrement** auquel vous accorderez l'accès.
5. Sélectionnez le **rôle cible** approprié.
6. Cochez la case Spécifier l'objectif et saisissez les détails de l'objectif dans les champs nouvellement affichés, comme suit :



- **Spécification de chiffrement** : sélectionnez la spécification de chiffrement à utiliser.
- **Opération granulaire** : sélectionnez Chiffrement symétrique dans la liste déroulante.

7. Sélectionnez la zone **Actif** .
8. Pour **Résultat** , sélectionnez **Suivre**.

Résultats

Le rôle granulaire MAP permet à un utilisateur qui n'est pas affecté à une MAP de soumettre des formulaires d'enregistrement public tout en sécurisant les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une politique de cycle de vie du module cryptographique

Créez une politique de cycle de vie du module de chiffrement pour imposer des limites aux modules de chiffrement, telles que la durée de conservation de la clé. Créez des politiques pour protéger les modules cryptographiques en limitant leur exposition.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Une politique de cycle de vie de module cryptographique est une politique au niveau de l'instance. Plus une clé cryptographique est exposée, plus elle risque d'être compromise. Protégez les clés en limitant la durée d'utilisation des clés et les personnes qui peuvent les utiliser.

Les fonctionnalités suivantes régissent les modules de chiffrement :

- Les politiques d'instance définissent des limites pour l'instance. Par exemple, si vous spécifiez dans une stratégie d'instance que la date d'expiration ne doit jamais être supérieure à deux ans après la date d'activation, vous ne pouvez pas utiliser les règles de cycle de vie pour définir une date d'expiration cinq ans après la date d'activation.

- Les modèles de cycle de vie d'instance vous permettent de définir différentes politiques pour différentes clés. Les modèles offrent des règles de cycle de vie par défaut pour les modules cryptographiques afin qu'il ne soit pas nécessaire de les recréer pour chaque module. Par exemple, vous pouvez définir des dates d'expiration différentes pour les clés de chiffrement de données symétriques et pour les clés d'encapsulation de clé publique.

- Les règles de cycle de vie affectent directement les clés. Par exemple, si vous spécifiez dans les règles de cycle de vie que la date d'expiration doit être de deux ans après la date d'activation, les clés expireront deux ans après la date d'activation.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Politiques de cycle de vie** > **Politiques d'instance**.
2. Sélectionner **Nouveau**.
3. Renseignez le formulaire.

   Champs des politiques du cycle de vie cryptographiques

Champ	Description
Concerne	Lecture seule. Clé à laquelle le cycle de vie s'applique.
Actif	Sélectionnez cette option pour activer la politique.
Condition de la politique	Instructions conditionnelles qui précisent quand activer, renouveler, désactiver et détruire le module de chiffrement.
Résultat	**Refuser** pour révoquer l'accès au module cryptographique ou **Suivre** pour autoriser l'accès et surveiller l'utilisation du module cryptographique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Si vous souhaitez ajouter des exceptions à cette politique de cycle de vie au niveau du module, reportez-vous à la section Créer des exceptions de politique de cycle de vie de module.

Créer des exceptions de politique de cycle de vie de module

Créez une exception de politique de module pour modifier la politique de cycle de vie d'une clé uniquement pour une clé spécifique sur une instance.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager et sn_kmf.admin

Les exceptions s'appliquent uniquement à ce module et non à l'ensemble de l'instance. Par exemple, un administrateur a configuré des clés symétriques pour qu'elles soient limitées à une année au niveau de l'instance. Une exception peut être faite au niveau du module pour être de deux ans.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Modules de chiffrement Tous**.
2. Sélectionnez le module de chiffrement qui utilisera les exceptions de politique.
3. Dans la table Module de chiffrement, sélectionnez l'icône **Exceptions de politique du module** onglet.
4. Sélectionner **Nouveau**.
5. Renseignez le formulaire.

Champs Exceptions de politique du module

Champ	Description
Module de chiffrement	Nom du module sélectionné. Ce champ est en lecture seule.
Concerne	La clé spécifiée est renseignée automatiquement.
Type de clé	Type de clé auquel les politiques d'exception sont associées. **Remarque :** Vous ne pouvez sélectionner qu'un seul type de clé, mais plusieurs politiques d'exception peuvent être créées par module de chiffrement.
Condition de la politique	Condition personnalisable qui détermine quand l'exception de politique s'applique.
Résultat	Résultat qui se produit lorsque la condition du champ **Condition de politique** est remplie. ○ **Rejeter** rejette l'utilisation de la clé. ○ **Track** permet d'utiliser la clé.

6. Sélectionner **Envoyer** à retourner à la table Module de chiffrement.

Référence du cadre de travail de gestion des clés

L'API Cadre de travail de gestion des clés /UX (KMF) vous permet de personnaliser et de gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow instance. Le fournit ServiceNow Cadre de travail de gestion des clés une interface sécurisée et complète pour les services de gestion des clés cryptographiques côté instance.

Cadre de travail de gestion des clés États clés du cycle de vie

KMF prend en charge plusieurs états du cycle de vie des clés cryptographiques grâce à l'application d'actions spécifiques autorisées. Par exemple, seules les clés qui sont à l'état actif peuvent être utilisées entièrement à leur fin cryptographique prévue. Le tableau suivant fournit plus de détails sur les différents états clés du cycle de vie.

Rôles installés avec Key Management Framework

Le Cadre de travail de gestion des clés (KMF) introduit des rôles spécifiques pour les configurations liées au module cryptographique et à la gestion des clés.

Visualisation de la politique d'accès au module

Utilisez la visualisation de la politique d'accès au module pour afficher toutes les informations pertinentes du module de chiffrement sur une seule page d'interface utilisateur.

Débogueur de politique d'accès au module

Utilisez le débogueur de politique d'accès au module pour examiner les informations de connexion et comprendre pourquoi vos utilisateurs ont accès ou non à un contexte de chiffrement.

Chiffrement et gestion des clés par lot

Avec la gestion des clés, Chiffrement de champ est mis à niveau sans frais supplémentaires vers les modules de chiffrement hautement configurables. Vous avez également la possibilité de passer à la licence d'utilisation illimitée. Abonnez-vous au nouveau lot d'autorisations de chiffrement, Chiffrement de plateforme, qui comprend Chiffrement de champ Enterprise et Chiffrement dans le cloud.

Cadre de travail de gestion des clés États clés du cycle de vie

KMF prend en charge plusieurs états du cycle de vie des clés cryptographiques grâce à l'application d'actions spécifiques autorisées. Par exemple, seules les clés qui sont à l'état actif peuvent être utilisées entièrement à leur fin cryptographique prévue. Le tableau suivant fournit plus de détails sur les différents états clés du cycle de vie.

État ou action du cycle de vie clé	Description
Actif	La clé active est utilisée pour générer de nouveaux contenus, tels que le chiffrement ou la signature. Il ne peut y avoir qu'une seule clé active pour une spécification cryptographique donnée dans un module cryptographique.
Compromis	Les clés compromises ne peuvent pas être utilisées pour générer de nouveau contenu, comme le chiffrement ou la signature, mais peuvent toujours être utilisées pour identifier l'objectif d'un contenu existant, comme le déchiffrement ou la vérification. Plusieurs clés peuvent exister à l'état compromis pour la révocation dans une spécification cryptographique donnée dans un module cryptographique. Toute clé active ou suspendue peut être déplacée vers un état compromis.
Désactivé	Toute clé active peut être désactivée. Il peut y avoir plusieurs clés à l'état désactivé pour une spécification de chiffrement donnée dans un module de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État ou action du cycle de vie clé	Description
	Par exemple, lorsque la clé est tournée, la clé active actuelle est désactivée. Les clés désactivées ne peuvent pas être utilisées pour générer du nouveau contenu, comme le chiffrement et la signature, mais peuvent toujours être utilisées pour identifier des objectifs de contenu existant, tels que le déchiffrement ou la vérification. **Remarque :** Les clés compromises et révoquées sont traitées comme des clés désactivées.
Détruit	Lorsqu'une clé est détruite, le matériel de clé est définitivement supprimé et ne peut plus être utilisé à des fins cryptographiques. Toute clé désactivée peut être détruite à l'aide de l'automatisation du cycle de vie lorsqu'elle n'a pas été utilisée dans la période désignée configurée. Il peut y avoir plusieurs clés à l'état détruit pour une spécification de chiffrement donnée dans un module de chiffrement. **Avertissement :** Les données associées à une clé détruite ne sont plus accessibles. Par conséquent, une extrême prudence doit être exercée lors de l'exécution d'une action de clé de destruction.
Généré	Plusieurs clés peuvent exister à l'état généré pour une spécification cryptographique donnée dans un module cryptographique. Une clé générée peut être passée à un état actif lorsqu'aucune clé active n'existe pour la spécification de chiffrement donnée. La première clé générée est automatiquement définie sur active. **Remarque :** Si le choix est de générer une nouvelle clé, une nouvelle clé est générée et rendue active même s'il existe des clés à l'état généré pour la spécification cryptographique donnée.
Renouvelé	Une clé active avec une date d'expiration peut être renouvelée autant de fois que vous le souhaitez pour prolonger la période de cycle de vie de la clé. **Remarque :** La différence entre la date d'activation et la date d'expiration est calculée et la date d'expiration est reportée de cette durée par rapport au jour en cours.
Reprendre	L'action d'interface utilisateur est disponible sur les clés suspendues pour les ramener à un état actif lorsqu'aucune autre clé active n'existe pour la spécification de chiffrement donnée.
Révoqué	Toute clé active ou suspendue peut être passée à l'état Révoqué. Les clés révoquées ne peuvent pas être utilisées pour générer du nouveau contenu, comme le chiffrement ou la signature, mais peuvent toujours être utilisées pour identifier l'objectif d'un contenu existant, comme le déchiffrement ou la vérification. Plusieurs clés dans un état révoqué peuvent exister pour une spécification cryptographique donnée dans un module cryptographique.

Traduction automatique

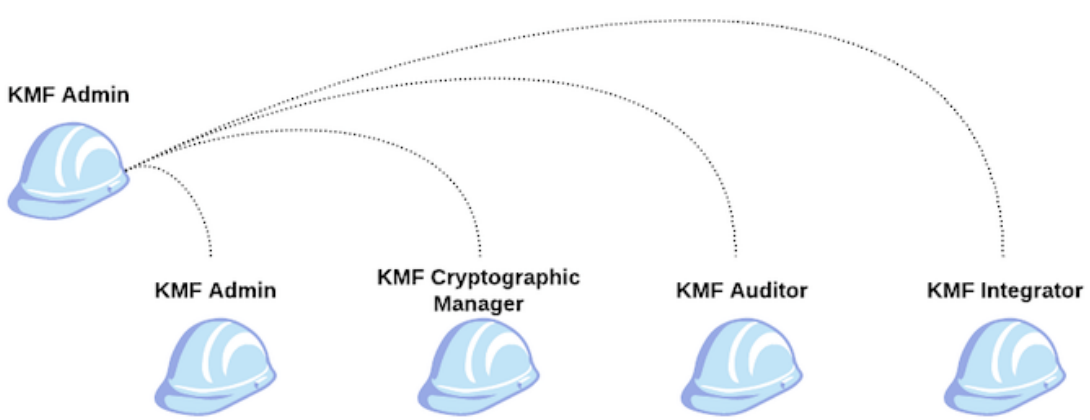
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État ou action du cycle de vie clé	Description
Pivoté	La rotation de clés entraîne la désactivation de la clé active actuelle et l'activation d'une autre clé. Sélectionnez la nouvelle clé active parmi les suivantes : • Génération d'une nouvelle clé. • Pointez sur une clé importée existante. Toute clé active peut être tournée.
Suspendu	Il peut y avoir plusieurs clés à l'état suspendu pour une spécification de chiffrement donnée dans un module de chiffrement. Lorsque la clé est suspendue, elle peut être reprise et réaffectée à un état actif lorsqu'aucune autre clé active n'existe pour cette spécification cryptographique.

Rôles installés avec Key Management Framework

Le Cadre de travail de gestion des clés (KMF) introduit des rôles spécifiques pour les configurations liées au module cryptographique et à la gestion des clés.

Important :
KMF rôles sont requis pour utiliser le Cadre de travail de gestion des clés. Les utilisateurs sans KMF rôles ne peuvent pas accéder aux listes, tables et modules utilisés pour configurer la gestion des clés.



Administrateur KMF [sn_kmf.admin]

Affecte des rôles à d'autres utilisateurs pour effectuer des opérations autour de ServiceNow Cadre de travail de gestion des clés.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Considérations spéciales

Important :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

- Ce rôle est affecté via le processus indiqué à la .Affecter des Cadre de travail de gestion des clés rôles
- Les utilisateurs ayant ce rôle doivent également avoir les fonctions administrateur et security_admin
- Vous devez disposer de ce rôle pour affecter des rôles KMF et exécuter en outre toutes les options du gestionnaire de chiffrement KMF.

Gestionnaire cryptographique KMF [sn_kmf.cryptographic_manager]

Créez, lisez et mettez à jour des opérations sur les modules cryptographiques (association de clés pour l'utilisation du chiffrement et les configurations d'algorithmes) et les politiques d'accès aux modules. En outre, les gestionnaires cryptographiques KMF peuvent effectuer la gestion des clés (générer, tourner, révoquer) et les opérations de cycle de vie.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Ce rôle peut uniquement être affecté à un utilisateur par un administrateur KMF.

Auditeur cryptographique KMF [sn_kmf.cryptographic_auditor]

Affichez les informations sur le module cryptographique, les métadonnées clés et les détails liés au cycle de vie, ainsi que les informations sur la politique d'accès au module (MAP).

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Ce rôle peut uniquement être affecté à un utilisateur par un administrateur KMF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrateur cryptographique KMF [sn_kmf.cryptographic_integrator]

Intégrez Cadre de travail de gestion des clés avec des magasins de clés ou des systèmes externes.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Ce rôle peut uniquement être affecté à un utilisateur par un administrateur KMF.

Opérateur de chiffrement KMF [sn_kmf.cryptographic_operator]

Accédez à une partie du ServiceNow Cadre de travail de gestion des clés cycle de vie clé : renouvellement, rotation, révocation.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations spéciales

Aucun.

Affecter des KMF rôles

Affectez KMF des rôles aux administrateurs, qui peuvent à leur tour affecter d'autres KMF rôles.

Avant de commencer
Rôle requis : admin et security_admin

Vous devez accéder au rôle security_admin avant d'affecter le KMF rôle administrateur. Pour obtenir des instructions, consultez Élever à un rôle privilégié

Procédure

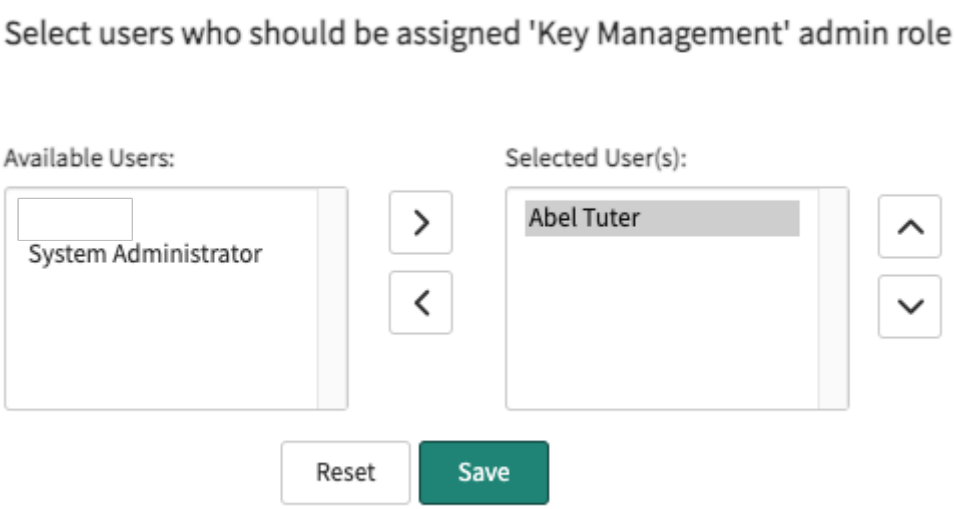
1. Accéder au rôle d'administrateur de sécurité.
2. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur dont vous souhaitez être l'administrateur KMF .
3. Vérifiez que l'utilisateur dispose déjà des rôles administrateur et security_admin.

Traduction automatique

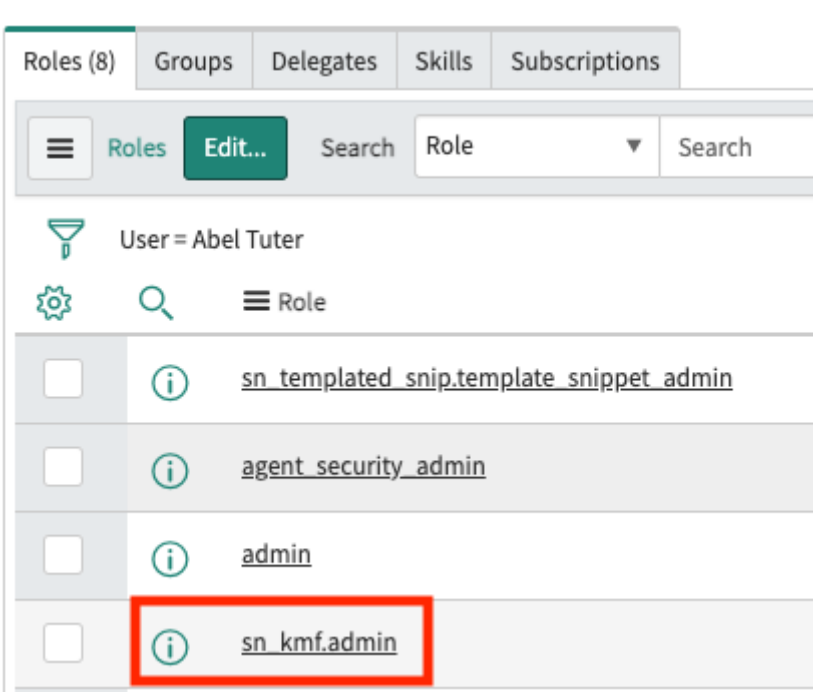
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si ce n’est pas le cas, sélectionnez **Modifier** sous la liste connexe Rôles et ajoutez des _admin **d’administrateur** et **de sécurité**.

4. Accédez à la **Sécurité de système** > **Administration de la gestion de clés**.
5. Sélectionnez l’utilisateur que vous souhaitez définir comme KMF administrateur dans la colonne **Utilisateurs disponibles** et déplacez-le vers la colonne **Utilisateurs sélectionnés** .



6. Sélectionnez **Enregistrer**.
7. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l’utilisateur à qui vous venez de donner le rôle sn_kmf.admin.
   L’utilisateur dispose du rôle sn_kmf.admin dans la liste connexe **Rôles** et peut affecter d’autres rôles KMF.



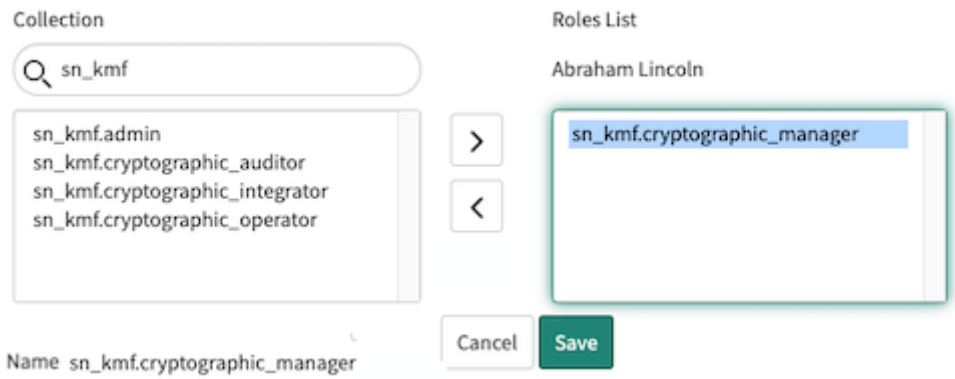
Que faire ensuite

Si vous disposez du rôle administrateur KMF, procédez comme suit pour affecter d’autres rôles KMF :

Traduction automatique

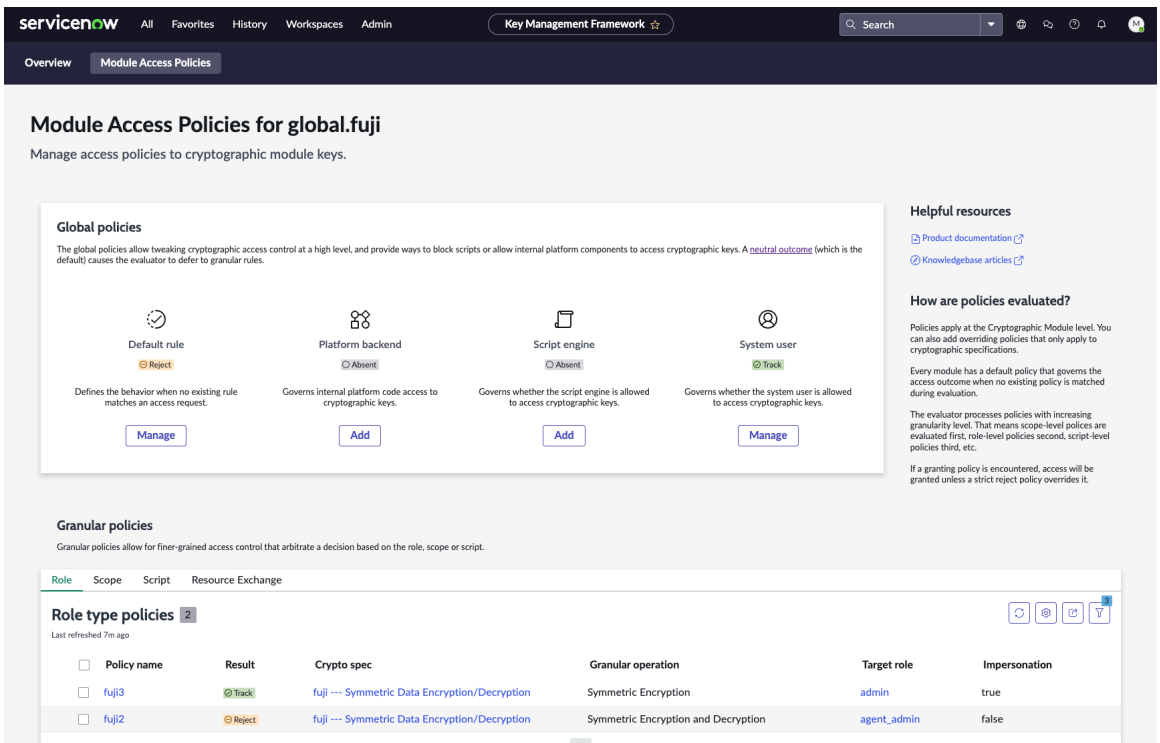
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur auquel vous souhaitez attribuer un autre rôle KMF, tel que Gestionnaire de chiffrement KMF.
2. Dans la liste connexe Rôles, sélectionnez **Modifier** et sélectionnez les rôles KMF que vous souhaitez affecter aux utilisateurs. Tous les rôles KMF commencent par `sn_kmf`.



Visualisation de la politique d'accès au module

Utilisez la visualisation de la politique d'accès au module pour afficher toutes les informations pertinentes du module de chiffrement sur une seule page d'interface utilisateur.



Les administrateurs de Key Management Framework et les gestionnaires de chiffrement peuvent utiliser la page d'interface utilisateur de politique d'accès au module pour afficher tous les mécanismes de contrôle d'accès liés à un module de chiffrement unique. Utilisez les informations collectées sur cette page de l'interface utilisateur pour déterminer qui a accès aux informations chiffrées sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les utilisateurs disposant des rôles OU *sn_kmf.cryptographic_manager* peuvent accéder à la page d'interface *sn_kmf.admin* utilisateur de visualisation de la politique d'accès au module en accédant à **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Tous**.

Étiquettes des résultats

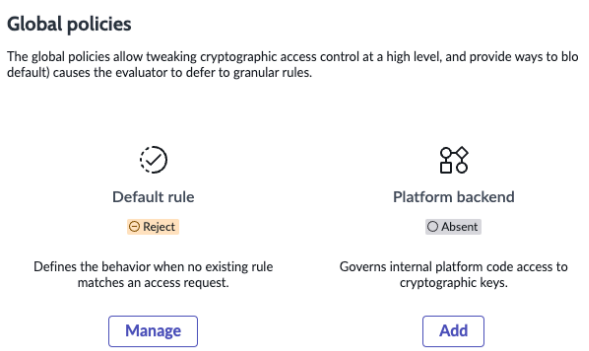
Les politiques d'accès au module contiennent un champ **Résultat** qui détermine s'il convient d'accorder l'accès au module cryptographique sélectionné. La page d'interface utilisateur affiche une étiquette sur les éléments de la page d'interface utilisateur en fonction de la valeur de ce champ.

Étiquette d'interface utilisateur	Valeur de champ de résultat	Définition
Track	*Track* ou *Allow*	L'accès est accordé à tous les utilisateurs, y compris aux scripts.
Reject	*Reject*	L'accès est refusé sauf si une politique d'accès au module de suivi est trouvée.
StrictReject	*StrictReject*	Accès refusé.
Absent	*N/A*	La politique d'accès au module n'existe pas sur l'instance. L'accès est refusé à tous.

Politiques globales

Utilisez la section **Politiques globales** pour examiner les politiques d'accès aux modules qui contrôlent l'accès au niveau de la plateforme.

Sélectionnez le bouton **Gérer** situé sous l'une des politiques pour accéder à cet enregistrement. Si la politique n'existe pas, un bouton **Ajouter** apparaît sous cette entrée. Sélectionnez le bouton **Ajouter** pour accéder à un nouvel enregistrement de politique dans lequel vous pouvez définir la politique.



Politique	Définition
Règle par défaut	La règle par défaut définit le comportement lorsqu'aucune règle existante ne correspond à une demande d'accès.

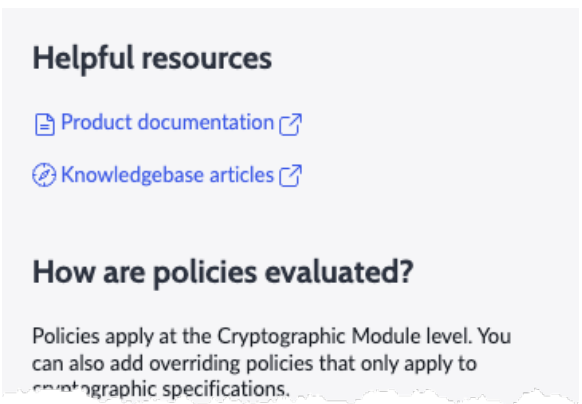
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique	Définition
Back-end de la plateforme	La politique back-end de la plateforme régit l'accès du code interne de la plateforme aux clés de chiffrement.
Moteur de script	La politique du moteur de script détermine si le moteur de script est autorisé à accéder aux clés de chiffrement.
Utilisateur système	La politique d'utilisateur système détermine si l'utilisateur système est autorisé à accéder aux clés de chiffrement.

Ressources utiles

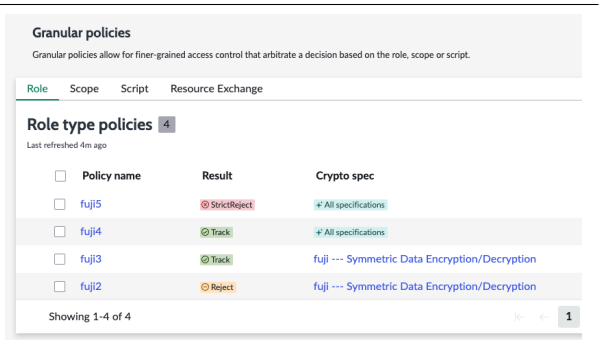
Utilisez la section **Ressources utiles** pour trouver des liens vers la documentation produit, des articles de la base de connaissances pertinents et une brève description de la façon dont les politiques d'accès aux modules sont évaluées sur la plateforme. Pour en savoir plus sur la façon dont les politiques d'accès aux modules sont évaluées, reportez-vous à la section Débogueur de politique d'accès au module.



Politiques granulaires

Utilisez la section **Politiques granulaires** pour afficher des listes de politiques d'accès au module, séparées par type de politique. Utilisez les onglets au-dessus de la liste pour sélectionner une catégorie de politique à afficher.

- Rôle
- Champ d'application
- Champ d'application et domaine (si Séparation en domaines est actif)
- Script
- Échange de ressources (si le module de chiffrement est un Password2 ou Chiffrement de champ un sous-module)
- Identité (si Secrets Management Enterprise est actif)



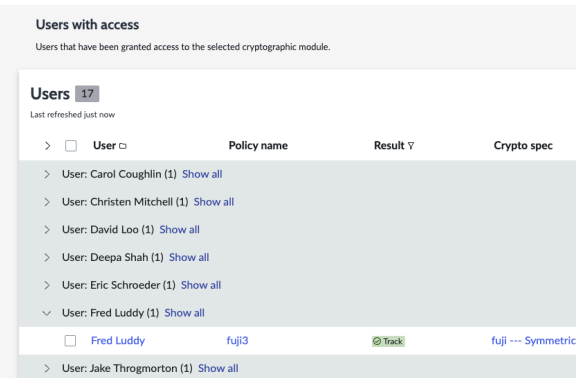
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, la liste each affiche uniquement les politiques actives. Utilisez l'icône de filtre pour modifier le filtre par défaut de la liste.

Utilisateurs ayant accès

Utilisez la section **Utilisateurs ayant accès** pour afficher une liste de tous les utilisateurs ayant accès au module de chiffrement sélectionné. La liste est regroupée par utilisateur, car un utilisateur unique peut posséder plusieurs rôles qui accordent l'accès à un module cryptographique.

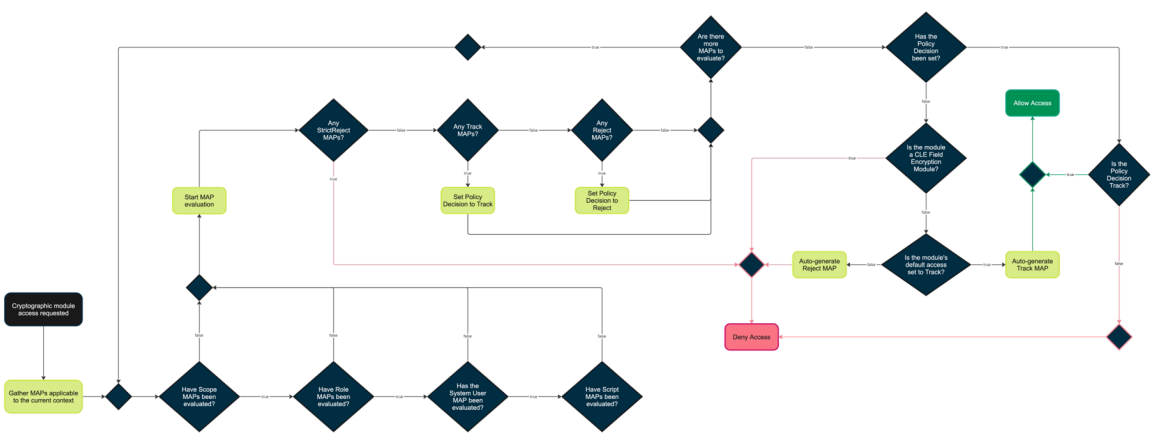


Débogueur de politique d'accès au module

Utilisez le débogueur de politique d'accès au module pour examiner les informations de connexion et comprendre pourquoi vos utilisateurs ont accès ou non à un contexte de chiffrement.

Les politiques d'accès au module (MAP) définissent les contrôles au niveau de l'instance pour l'accès aux modules cryptographiques. Les appelants (par exemple, un utilisateur ou un script) ont besoin d'un accès explicite pour utiliser un module cryptographique à des fins de chiffrement et de déchiffrement. Utilisez le débogueur pour voir quelles politiques sont évaluées lorsqu'un appelant tente d'accéder à un module de chiffrement. Vous pouvez également utiliser le débogueur et savoir pourquoi l'accès est accordé ou non.

Cet organigramme montre comment votre instance évalue les demandes d'accès à un module cryptographique.



Contrôler l'accès aux journaux de débogage

L'accès aux journaux de débogage d'accès au module est déterminé par rôle. Les utilisateurs disposant des `sn_kmf.admin` rôles et `sn_kmf.cryptographic_manager` ont accès au débogueur. Accorder l'accès à d'autres rôles à l'aide de la `glide.kmf.module_access_policies.debugger.authorized.roles` propriété système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La valeur de cette propriété est une liste séparée par des virgules des rôles qui accèdent aux journaux de débogage.

Activer ou désactiver le débogueur

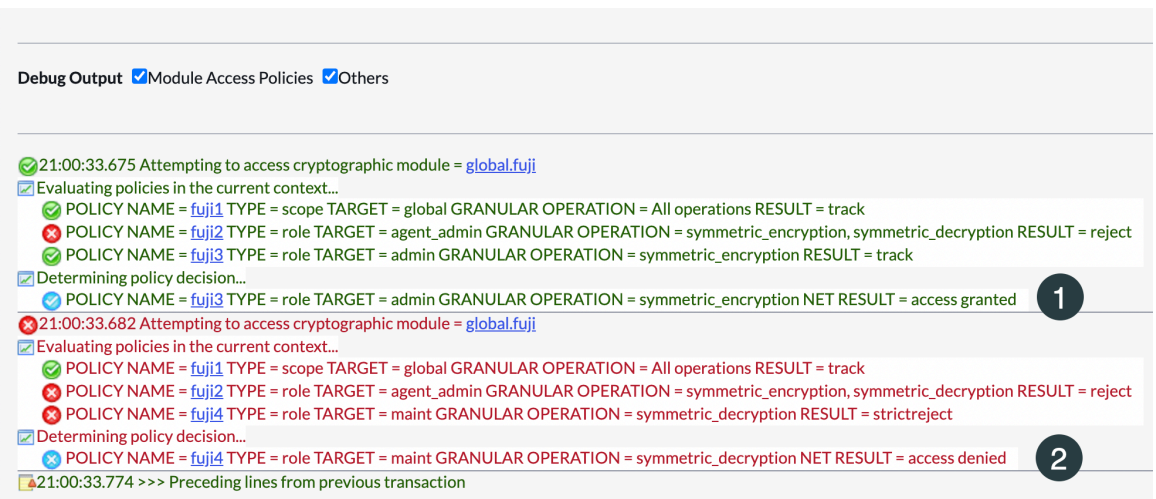
Pour activer les messages de journalisation de débogage pour les politiques d'accès au module, accédez à **Tous** > **Diagnostics** > **Débogage de session** > **Débogage pour les politiques d'accès au module** > **.**

Une fois le débogage terminé, vous pouvez désactiver les messages de journalisation en accédant à **Tous** > **Diagnostics** > **Débogage de session** > **Désactiver tout** > **.**

Accéder aux journaux

Après avoir activé le débogage, accédez à une page qui déclenche une évaluation MAP pour afficher les journaux de débogage MAP. Les messages de débogage s'affichent en bas de la page.

Conseil :
Vous pouvez utiliser l'emprunt d'identité pour résoudre les problèmes d'accès pour d'autres utilisateurs. Pour en savoir plus sur l'emprunt d'identité, reportez-vous à la section Impersonating users . Pour afficher les journaux de débogage du point de vue d'un autre utilisateur, assurez-vous que le champ **Emprunt d'identité**`role` de vos politiques d'accès au module est défini sur **vrai**.



Dans cet exemple, un appelant appelle deux demandes d'accès au module de chiffrement `global.fuji` . Un chiffrement symétrique, qui est accordé, et un déchiffrement symétrique, qui a été refusé.

Présentation des entrées de journal

Les informations de débogage sont structurées selon ce format.

1. Cette première ligne affiche le module cryptographique qui reçoit la demande d'accès.
2. Les lignes entre la première et la dernière ligne affichent les MAP évaluées dans l'ordre dans lequel elles ont été évaluées et incluent leur nom, leur type, leur cible, leur opération granulaire et leur résultat.
3. La dernière ligne affiche la décision de politique (le cas échéant) et le résultat de l'accès net pour l'appelant (si l'accès est accordé à l'appelant).

Chaque ligne commence par une icône qui indique son type de message.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Icônes de messages

Icône	Type du message
	Message d'information
	La politique d’accès au module accorde l’accès
	Politique d’accès au module : refus d’accès
	L’accès est accordé à l’appelant
	L’accès est refusé à l’appelant
	Aucune politique d’accès au module à évaluer

Exemples de journaux de débogage

Message d’accès accordé

21:24:32.564 Attempting to access cryptographic module = global.fuji
Evaluating policies in the current context...
POLICY NAME = fuji1 TYPE = scope TARGET = global GRANULAR OPERATION = All operations RESULT = track
POLICY NAME = fuji2 TYPE = role TARGET = agent_admin GRANULAR OPERATION = symmetric_encryption, symmetric_decryption RESULT = reject
POLICY NAME = fuji3 TYPE = role TARGET = admin GRANULAR OPERATION = symmetric_encryption RESULT = track
Determining policy decision...
POLICY NAME = fuji3 TYPE = role TARGET = admin GRANULAR OPERATION = symmetric_encryption NET RESULT = access granted

Message d’accès refusé

21:24:32.574 Attempting to access cryptographic module = global.fuji
Evaluating policies in the current context...
POLICY NAME = fuji1 TYPE = scope TARGET = global GRANULAR OPERATION = All operations RESULT = track
POLICY NAME = fuji2 TYPE = role TARGET = agent_admin GRANULAR OPERATION = symmetric_encryption, symmetric_decryption RESULT = reject
POLICY NAME = fuji4 TYPE = role TARGET = maint GRANULAR OPERATION = symmetric_decryption RESULT = strictreject
Determining policy decision...
POLICY NAME = fuji4 TYPE = role TARGET = maint GRANULAR OPERATION = symmetric_decryption NET RESULT = access denied

Accès refusé (aucune politique d’accès au module à évaluer

21:40:46.124 Attempting to access cryptographic module = global.fuji
Evaluating policies in the current context...
There are no policies to evaluate in the current context
Determining policy decision...
NET RESULT = access denied

Accès refusé (privilèges insuffisants)

21:44:36.597 Insufficient privileges. You do not have permission to access the Module Access Policies evaluation logs. Contact your KMF admin or cryptographic manager. Please refer to the following knowledge base article: KB1294649

Chiffrement et gestion des clés par lot

Avec la gestion des clés, Chiffrement de champ est mis à niveau sans frais supplémentaires pour inclure des modules de chiffrement hautement configurables. Vous pouvez également effectuer une mise à niveau vers la licence à utilisation illimitée. Abonnez-vous au nouveau lot d’autorisations de chiffrement, Chiffrement de plateforme, qui comprend Chiffrement de champ Enterprise et Chiffrement dans le cloud.

Fonctionnalités de Chiffrement de champ

Chiffrement de champ avec modules de chiffrement est inclus gratuitement dans votre instance et inclut la gestion des clés NIST 800-57 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Fonctionnalités du groupe Chiffrement de la plateforme

Le groupe Chiffrement de la plateforme ajoute les fonctionnalités et offres suivantes :

- Chiffrement.
- Chiffrement dans le cloud avec gestion des clés.

Informations supplémentaires

Pour en savoir plus sur la gestion des clés, reportez-vous à la section Explorer le cadre de gestion des clésExplorer le cadre de gestion des clés.

Actions de gestion des clés

L'une des principales fonctionnalités de KMF est de fournir la possibilité de gérer les clés, telles que la révocation ou la rotation des clés. KMF sécurise correctement les données sensibles avec les matériaux de chiffrement et les opérations de cycle de vie les plus récents.

Le tableau suivant fournit un résumé des principales opérations et actions de gestion du cycle de vie. L'objectif du module de chiffrement est appliqué aux données avec la configuration du module de chiffrement et n'a aucun impact sur les données.

Action de gestion des clés	Description
Générer la clé	Génère une nouvelle clé pour le module de chiffrement donné. Une première clé générée est définie sur `active`.
Faire pivoter la clé	Désactive la clé actuelle et en génère une nouvelle. La nouvelle clé de module est définie sur current (active).
Révoquer la clé	Marque la clé actuelle et l'état du cycle de vie comme révoqués. Le module de chiffrement génère automatiquement une nouvelle clé sur de nouvelles données et définit l'état de la clé sur actif. Révoqué signifie que la clé n'est plus utilisée pour le chiffrement. Cependant, il peut toujours être utilisé pour le déchiffrement. Vous ne pouvez pas détruire une clé.
Suspendre la clé	Marque la clé actuelle comme suspendue. Reprenez manuellement la clé suspendue ou révoquez la clé suspendue pour générer une nouvelle clé de module avant d'utiliser à nouveau le module de chiffrement.
Reprendre la clé	Marque une clé suspendue comme clé active.
Renouveler la clé	Prolonge la durée de vie de la clé actuelle. Le bouton **Renouveler** devient disponible dans les circonstances suivantes : • Le rôle de gestionnaire cryptographique vous est affecté. • L'état du cycle de vie est marqué sur **Actif** ou **Renouvelé**. • Une date d'expiration est définie dans la définition du cycle de vie du module.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher et gérer les clés

Examinez l'état de n'importe quelle clé pour déterminer d'autres actions clés, telles que le moment du renouvellement, de la rotation, de la suspension, de la désactivation ou de la destruction d'une clé actuelle.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez un module de chiffrement.

   Le formulaire Module de chiffrement <nom-module> s'affiche.
3. Dans l'onglet Clés de module, sélectionnez l'alias de clé pour examiner l'état de la clé sur le formulaire de cycle de vie <nom de la clé>.
4. Examinez le formulaire, car tous les champs sont en lecture seule.

Cycle de vie cryptographique Champs clés

Champ	Description
Date de création	Affiche la date à laquelle la clé a été générée.
Date d'activation	Affiche la date à laquelle la clé a été activée.
Dernière date de renouvellement	Affiche la date du dernier renouvellement de la clé.
Date de la dernière rotation	Affiche la date de la dernière rotation de la clé.
Date de désactivation	Affiche la date à laquelle la clé a été désactivée.
Date de destruction	Affiche la date à laquelle la clé a été détruite.
État du cycle de vie de la clé	Affiche l'état clé du cycle de vie.
Prochaine date d'activation	Affiche la date future d'activation de clé.
Prochaine date de renouvellement	Affiche la date future de renouvellement des clés.
Prochaine date de rotation	Affiche la date future de la rotation de clés.
Prochaine date de destruction	Affiche la date future à laquelle la clé est détruite.
Date d'expiration	Affiche la date à laquelle la clé expire.

5. Pour effectuer une action sur la clé, sélectionnez l'une des options suivantes pour prendre effet immédiatement :
   - **Révoquer la clé**: sélectionnez cette option pour désactiver la clé et générer une nouvelle clé. Entrez la raison pour laquelle vous révoquez la clé.
   - **Faire pivoter la clé**: sélectionnez cette option pour désactiver la clé actuelle et générer une nouvelle clé à sa place. La nouvelle clé est répertoriée dans la table Clé de module et le numéro de version de la clé est incrémenté de 1. Consultez la section pour en savoir plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Suspendre la clé**: sélectionnez cette option pour désactiver la clé actuelle.
- **Reprendre la clé** : sélectionnez cette option pour marquer une clé suspendue comme clé active. Cette option n'est disponible qu'après la suspension de la clé active.

Faire pivoter les clés

Pour une sécurité accrue, vous pouvez faire tourner vos clés cryptographiques selon un calendrier prédéterminé. La rotation de clés consiste à mettre hors service une clé de chiffrement et à remplacer cette ancienne clé par la génération d'une nouvelle clé de chiffrement.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

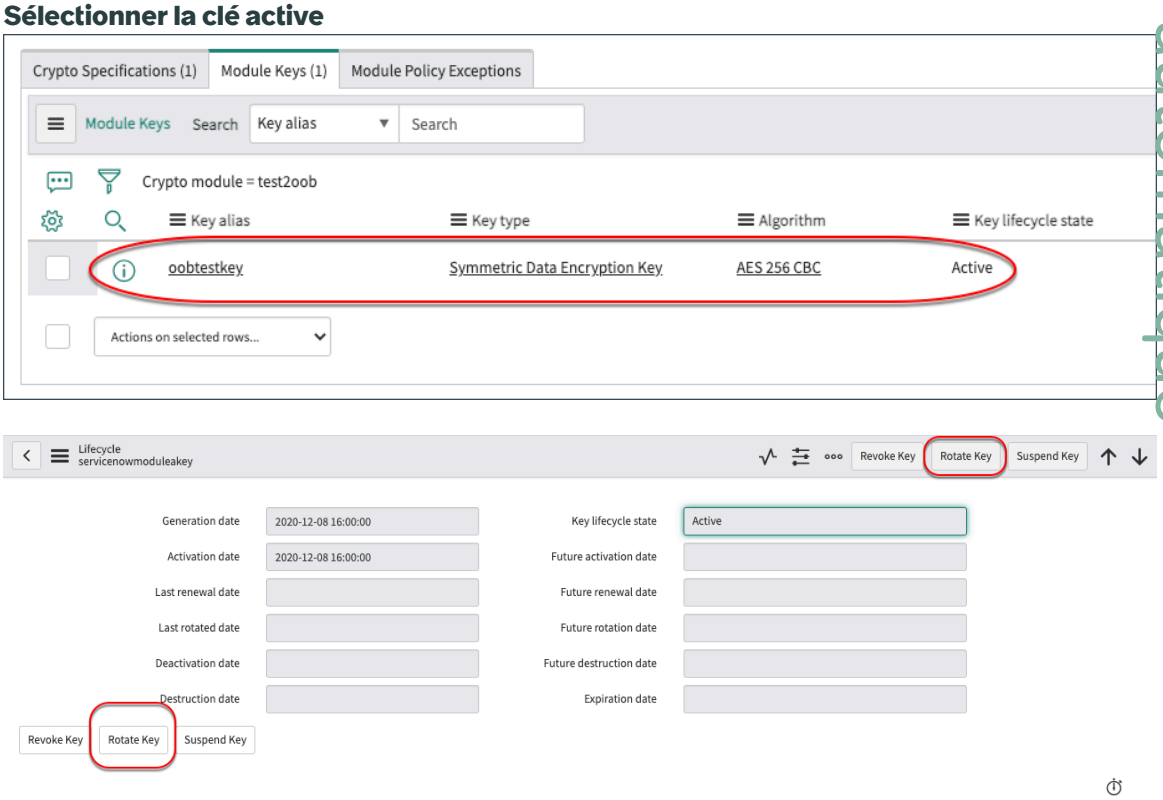
Pourquoi et quand exécuter cette tâche

Les modules de chiffrement, contrairement aux contextes de chiffrement, prennent en charge une nouvelle saisie des enregistrements pour un nouveau chiffrement avec une nouvelle clé. Ce qui suit montre comment effectuer une opération de rotation de clé manuellement sur un module cryptographique.

Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module cryptographique pour la rotation de clé.
3. Dans l'onglet **Clés du module** , sélectionnez la clé Actif.

Sélectionner la clé active

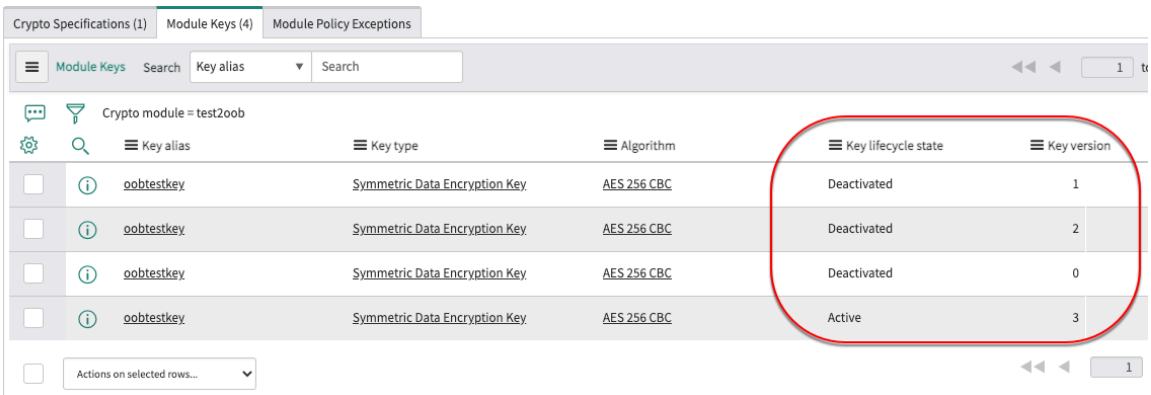


4. Sélectionnez **Faire pivoter la clé**.
   L'état du cycle de vie de la clé devient « Désactivé ». Les champs **Date de la dernière rotation**, **Date de désactivation** et **Version de clé** sont mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Retourner à **Module de chiffrement** > **Clés de module**.



Une clé de module supplémentaire est répertoriée dans la table. La touche nouvellement tournée devient « Actif » et la dernière touche est « Désactivée ».

Importer une clé à partir d'un service Web

Chargez en toute sécurité une clé client externe sur votre instance à l'aide de l'importation d'une clé à partir d'un service Web (par exemple, la clé REST API). Les clés publiques symétriques et asymétriques peuvent être importées dans un module cryptographique ciblé KMF .

La clé à importer (la clé cible) doit être chiffrée avec une clé d'emballage avant d'être chargée dans le module de chiffrement cible de l'instance. Cette clé d'encapsulation est le composant public d'une paire de clés publique/privée, qui doit être présente sur l'instance. La clé est une condition préalable pour que la clé cible encapsulée puisse être chargée via l'importation à partir de services Web.

Ces deux procédures distinctes (importation de la paire de clés d'encapsulation et importation de la clé cible encapsulée à partir d'un service Web) sont détaillées dans la documentation suivante. Cette paire de clés doit être générée et chargée pour être disponible dans le module de chiffrement d'importation de clé interne de l'instance.

Remarque :
Cet exemple utilise OpenSSL pour la génération de clés et de certificats et l'outil de test d'API Postman pour montrer l'utilisation de l'API REST. Remplacez d'autres outils comparables en fonction des besoins de votre entreprise.

Importer la paire de clés d'encapsulation/de désencapsulation

Configurez Cadre de travail de gestion des clés les paramètres d'importation avant d'importer une clé.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche
Cet exemple utilise OpenSSL pour la génération de clés et de certificats. Remplacez d'autres outils comparables en fonction des besoins de votre entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

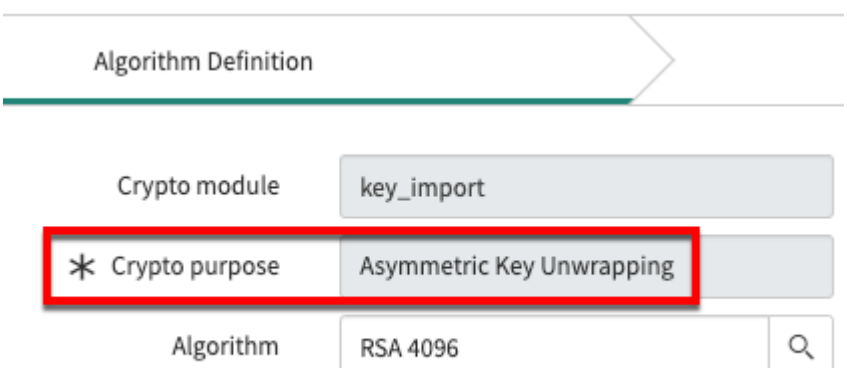
1. Dans votre environnement local, utilisez le terminal pour créer un certificat.
   Par exemple : `openssl req -x509 -sha256 -nodes -days 365 -newkey rsa :4096 -keyout wrapping_private.key -out wrapping_public.crt`

   Ce certificat est un composant public qui contient une clé. Le certificat est utilisé pour encapsuler une clé symétrique AES.

2. Dans votre environnement local, utilisez le terminal pour créer un magasin de clés contenant un certificat public (avec la clé d'emballage) et une clé de désencapsulation privée.
   Par exemple :`openssl pkcs12 -export -in wrapping_public.crt -inkey wrapping_private.key -name « wrapping_key_alias » -out wrapping_keystore.p12`

3. Sur votre instance, accédez à **Tous** > **Gestion des clés** > **Paramètres d'importation** > **Paramètres d'importation de clé**.

4. Dans la section Définition de l'algorithme, vérifiez que **l'objectif de chiffrement** est défini sur *`Désencapsulation de clé asymétrique`*.



5. Sélectionnez un algorithme approprié qui s'aligne sur le matériel de clé asymétrique pour le magasin de clés importé.
   Consultez Vue d'ensemble des spécifications cryptographiques pour plus d'informations.

6. Sélectionnez **Suivant**.

7. Dans la section **Définition du cycle de vie** , sélectionnez **Suivant** pour continuer.

8. Dans la section **Origine** de la clé, sélectionnez **Importer à partir de PKCS12** ou **Importer à partir de BCFKS** dans le champ **Origine** .

   Remarque :
   Si vous utilisez l'exemple de magasin de clés de l'étape 1, sélectionnez **Importer à partir de PKCS12**.

9. Entrez un **alias de clé** pour identifier la clé.
   Cet alias doit correspondre à l'alias de clé (ou « nom convivial ») qui a été spécifié lors de la génération du certificat ou du magasin de clés à télécharger. En poursuivant l'exemple ci-dessus, ce serait `wrapping_key_alias`.

10. Sélectionnez **Suivant**.
    La section **Création de clé** inclut un lien **Importer la clé** , qui affiche une boîte de dialogue pour charger le magasin de clés. En continuant l'exemple, ce serait `wrapping_keystore.p12`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer une clé encapsulée à partir d'un service Web

Chargez votre clé encapsulée dans un module cryptographique à l'aide de la fonctionnalité d'importation de clé à partir du service web. L'exemple utilise une clé symétrique. Des étapes similaires peuvent être utilisées pour importer une clé asymétrique.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager (configuration du module), sn_kmf.cryptographic_operator (authentification de base de l'opération REST)

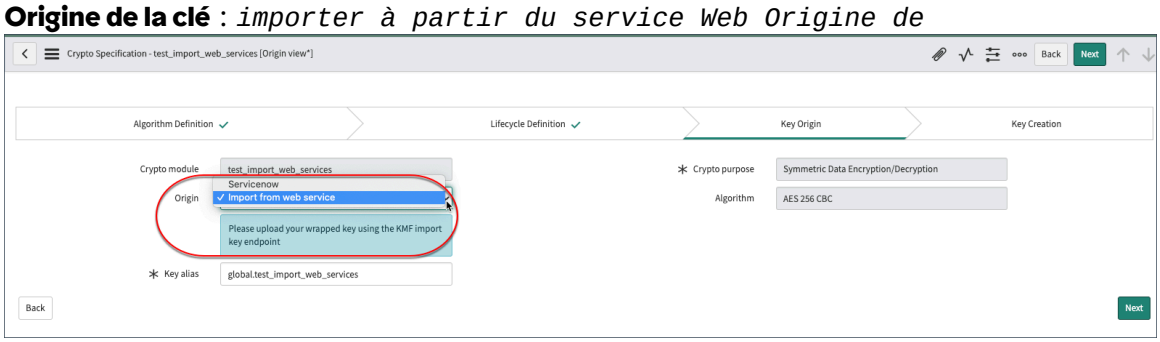
Pourquoi et quand exécuter cette tâche

KMF L'accès au point de terminaison de la clé d'importation est requis pour terminer le processus d'importation de la clé.

Cet exemple utilise OpenSSL pour générer des clés et des certificats. Vous pouvez remplacer d'autres outils comparables en fonction de vos besoins.

Procédure

1. À l'aide du terminal de votre périphérique local, encapsulez votre clé symétrique à l'aide de la clé d'encapsulation de clé publique du module d'importation de clés.
   Par exemple : `openssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_padding_mode :oaep -pkeyopt rsa_oaep_md :sha256 -out wrapped_symmetric_key.txt`
   Cet exemple crée un fichier de clé encapsulée nommé `wrapped_symmetric_key.txt`.
2. Créez un module cryptographique à lier à l'API.
   Voir ou pour plus d'informations.
3. Ajoutez une spécification cryptographique avec les sélections suivantes.
   - **Objectif de chiffrement** : *`chiffrement/déchiffrement de données symétriques`*.
   - **Origine de la clé** : *`importer à partir du service Web Origine de`*



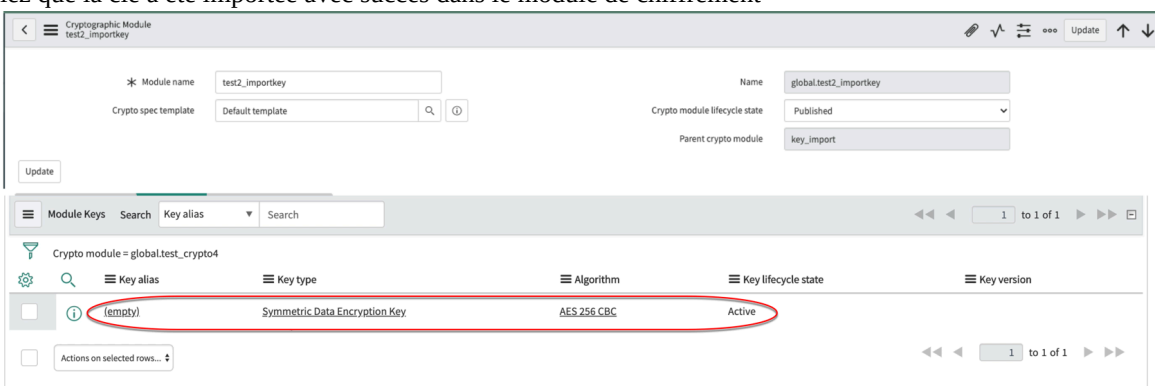
   Consultez ou pour plus d'informations.
4. Exécutez une *`demande HTTP POST`* à l'importation à partir d'un point de terminaison REST de service Web.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’importation réussie de la clé publique entraîne un message de réponse HTTP avec `l’état 200`.

5. Vérifiez que la clé a été importée avec succès dans le module de chiffrement ciblé.



Intégrité de Key Management Framework

Accédez à des informations sur l’état d’intégrité sur demande pour le Cadre de travail de gestion des clés. Les erreurs d’avertissement et de dysfonctionnement contiennent un message détaillé.

Avant de commencer

Rôle requis : sn_kmf_cryptographic auditeur, sn_kmf_admin ou sn_kmf_cryptographic_manager

Pourquoi et quand exécuter cette tâche

Chaque composant de la Cadre de travail de gestion des clés est décrit et signale les états et couleurs suivants :

- Vert/Opérationnel : Le composant est opérationnel, aucune erreur à signaler.
- Gris/Désactivé : le composant est inactif, par conséquent aucune vérification de l’intégrité n’est effectuée.
- Jaune/Dégradé : Avertissement, le composant fonctionne, mais des retards/problèmes temporaires sont susceptibles de se produire.
- Rouge/Dysfonctionnement : une erreur fatale empêche le composant de fonctionner, ce qui est susceptible de provoquer des pannes partielles.

Les composants peuvent inclure des sous-composants avec des rapports individuels et leur propre état d’intégrité impacte le parent comme suit :

- Si tous les sous-composants sont inactifs, le parent s’affiche comme inactif. Les sous-composants inactifs n’ont pas d’impact sur la santé de leurs parents.
- Si un ou plusieurs sous-composants sont dégradés ou défectueux, l’intégrité parent s’affiche comme dégradée.
- Si tous les sous-composants signalent un dysfonctionnement, le parent le signale également.

Pour plus d’informations sur les sous-composants, reportez-vous à la section Clés au niveau de l’instance dans le cadre de travail de gestion des clés.

Remarque :
Les vérifications de l’intégrité s’exécutent toutes les 15 secondes. Actualisez la page d’intégrité pour réexécuter le rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > > **Diagnostics**.
2. Examinez les renseignements suivants sur l'état de santé :

Informations de diagnostic

Catégorie	Détails
Clé sécurisée	Vérifie si le chiffrement est en cours de tentative.
Magasin de clés de fichier	Vérifie si une tentative d'extraction de clé racine d'instance (IRK) est en cours. **Remarque :** Le magasin de clés de fichier est une alternative hors ligne à Key Secure utilisée pour les instances sur site et les instances de développeur.
GlideEncrypter	Vérifie si un module de chiffrement, une spécification et une clé au niveau de l'instance GlideEncrypter sont présents. **Remarque :** GlideEncrypter est un composant scriptable qui permet un chiffrement transparent des champs et d'autres utilisations de Password2 chiffrement héritées via le Cadre de travail de gestion des clés.
Clé de chiffrement de clé d'instance (IKEK)	Vérifie si la clé peut être extraite à partir du magasin de clés de fichier ou de KeySecure.
Clé HMAC d'instance	Vérifie si la clé peut être extraite à partir du magasin de clés de fichier ou de KeySecure.
PKI du coffre-fort	Vérifie la connectivité du coffre-fort pour vérifier si la clé de chiffrement asymétrique d'instance (IAEK) et la clé de signature d'instance (ISK) sont utilisables et peuvent être extraites du coffre.
EJBCA PKI	Vérifie la connectivité LDAP pour vérifier si IAEK et ISK sont utilisables et peuvent être extraits du cache et LDAP.
PKI d'instance	Recherche une clé dans le magasin de clés de fichier et KeySecure et vérifie si le certificat est présent et correspond à la clé symétrique. **Remarque :** L'instance PKI n'est disponible que sur les instances situées au sein d'un ServiceNow centre de données.

Pour obtenir de l'aide sur le dépannage, contactez Service client et assistance.

Préparer votre instance à l'obsolescence de GlideEncrypter

Utilisez un script d'analyse d'instance pour trouver et supprimer les appels d'API GlideEncrypter sur votre instance. La suppression de ces appels est une étape nécessaire pour déconseiller le chiffrement 3DES sur votre instance.

Avant de commencer

Rôle requis : admin

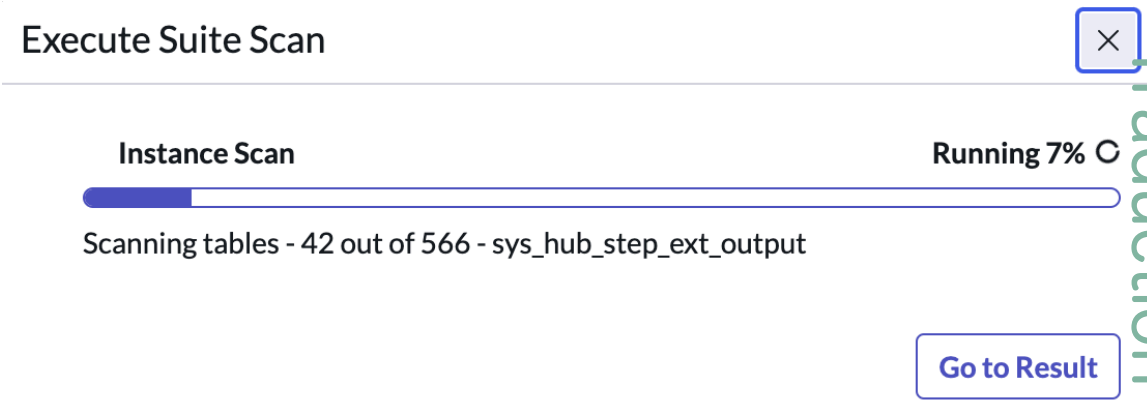
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'API GlideEncrypter devrait être obsolète à partir de la version zurichoise de ServiceNow. La suppression des appels GlideEncrypter de votre script est également une étape nécessaire avant de déconseiller le chiffrement 3DES sur votre instance.

Procédure

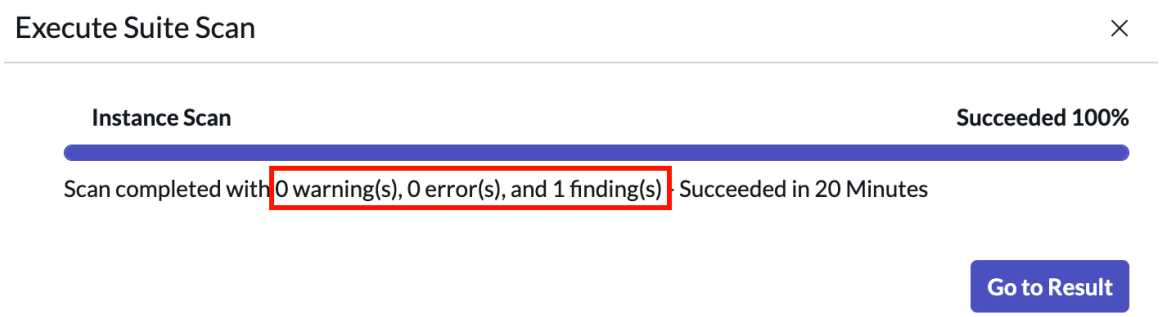
1. Accédez à la **Tous** > **Instance Scan** > **Suites**.
2. Dans la liste **Suites** , sélectionnez **GlideEncrypter** pour identifier les enregistrements utilisés par GlideEncrypter.
3. Dans l'enregistrement **Suites** , sélectionnez **Exécuter l'analyse de la suite**.
4. Dans la fenêtre **Analyser les suites maintenant** , sélectionnez **Instance complète**, puis **Exécuter l'analyse**.
   L'analyse de la suite s'exécute. Pendant l'exécution d'une **analyse de test d'exécution**, une fenêtre affiche la progression de



   l'analyse.

   Remarque :
   Cette analyse vérifie uniquement les enregistrements qui ont été créés ou modifiés par le client.

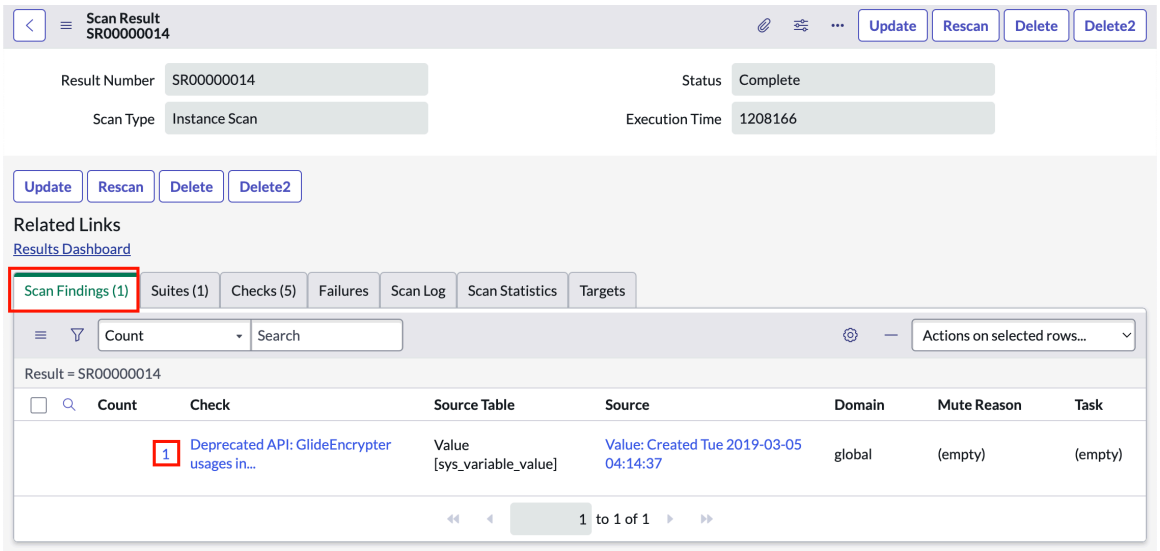
5. Lorsque l'analyse est terminée, sélectionnez **Accéder au résultat** pour afficher l'enregistrement du **résultat de l'analyse** .



6. Dans l'enregistrement **du résultat de l'analyse** , sélectionnez le champ **Nombre** de la liste Conclusions de **l'analyse** pour accéder à un enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Modifiez tous les scripts dans l'enregistrement qui utilisent l'API **GlideEncrypter** .
   Pour plus de détails sur les alternatives à **GlideEncrypter**, consultez Alternatives aux API GlideEncrypter déconseillées .
8. Après avoir supprimé les appels **GlideEncrypter** de vos scripts, exécutez à nouveau l'analyse pour vous assurer qu'il n'y a pas d'appels restants à l'API.

Que faire ensuite

Déconseiller l'utilisation de GlideEncrypter de 3DES pour les champs password2

Dépréciation de GlideEncrypter

Découvrez comment supprimer les appels GlideEncrypter hérités des scripts sur votre instance.

Disponibilité de GlideEncrypter dans la Zurich version

La disponibilité de GlideEncrypter dans la Zurich version varie selon que votre instance a été créée ou mise à niveau à partir d'une version précédente.

Nouvelles instances

Cette API est désactivée par défaut dans les nouvelles instances créées dans Zurich ou ultérieurement. Tous les scripts du système de base ont été mis à jour et n'utilisent plus d'appels à cette API.

Instances mises à niveau

Zurich les instances qui ont été mises à niveau à partir d'une version précédente peuvent toujours utiliser l'API GlideEncypter héritée, mais l'API a été mise à jour pour utiliser le chiffrement AES256-GCM via le Key Management Framework. Ce changement remplace l'utilisation de la norme de chiffrement 3DES héritée pour se conformer aux directives du NIST, tout en permettant à tous les scripts utilisant encore GlideEncrypter de fonctionner.

Activer ou désactiver GlideEncrypter

La disponibilité de GlideEncrypter est contrôlée par la `glide.security.glideencrypter.allow` propriété système. Cette propriété système est définie sur **false** par défaut dans les nouvelles Zurich instances et ne peut pas être mise à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

jour. Dans les instances mises à niveau vers Zurich, cette propriété peut être changée par les administrateurs disposant du rôle security_admin.

La propriété système glide.security.glideencrypter.allow

Valeur	Comportement
vrai	Si la valeur est true, GlideEncypter peut toujours être appelé dans les scripts, mais il utilise le chiffrement AES256-GCM via l'option Key Management Framework.
Faux	Si la valeur est « faux », GlideEncrypter appelle « null » et les administrateurs voient cette erreur : `Unsupported call to GlideEncrypter. Details: GlideEncrypter is deprecated and now returns null, please refer KB1320986`

Déconseiller l'utilisation de GlideEncrypter de 3DES pour les champs password2

Déconseillez l'utilisation de la norme de chiffrement 3DES par GlideEncrypter sur votre instance. Assurez-vous que votre instance utilise l'AES (Advanced Encryption Standard) plus sécurisé exclusivement pour le chiffrement et le déchiffrement de vos données Password2.

À partir de , Rome les données password2 sont protégées à l'aide de la Cadre de travail de gestion des clés commande , qui utilise l'algorithme AES (Advanced Encryption Standard) plus moderne. Toutefois, certaines configurations et solutions de secours dans la logique password2 peuvent toujours utiliser l'algorithme 3DES pour le chiffrement et le déchiffrement.

Dans la version, les Vancouver administrateurs peuvent choisir de déconseiller entièrement l'algorithme 3DES. Une fois ce changement effectué, votre instance utilise le chiffrement AES exclusivement pour toutes les tâches de chiffrement et de déchiffrement relatives aux données password2. Ce changement offre une meilleure sécurité d'instance que le chiffrement 3DES et est nécessaire pour rester conforme au NIST.

Considérations avant l'obsolescence

Transfert de données password2 entre les instances

Lors du transfert de textes chiffrés password2 vers d'autres instances, vous devez vous assurer que est KMF Key Exchange activé entre les instances source et cible. Cette configuration garantit que les clés utilisées pour chiffrer les textes password2 sont disponibles sur les deux instances pour déchiffrer les textes chiffrés par password2. Avant de déconseiller 3DES, tenez compte des cas d'utilisation suivants qui peuvent avoir un impact sur les données password2 entre les instances.

- Si vous avez des applications sur votre instance qui utilisent des données password2, assurez-vous qu'elles KMF Resource Exchange sont installées sur cette instance. KMF Resource Exchange Garantit que les clés au niveau de l'instance utilisées pour chiffrer les données password2 sur l'instance source sont disponibles sur les instances cibles pour le déchiffrement. Pour plus d'informations, consultez Échange de ressources du cadre de travail de gestion des clés.
- Si vous prévoyez d'exporter des données password2 via XML ou des sources de données, assurez-vous que l'instance cible est KMF Key Exchange activée. Cette configuration garantit que les clés au niveau de l'instance utilisées pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

chiffrer les données password2 sur l'instance source sont disponibles sur les instances cibles pour le déchiffrement. Pour plus d'informations sur cette configuration, reportez-vous à la section Cadre de travail de gestion de clés Échange de clés.

Important :
Les exemples ci-dessus sont des scénarios plus courants, mais si vous utilisez d'autres moyens de transférer du texte chiffré password2 entre les instances, vous devez configurer KMF Resource Exchange pour vous assurer que l'instance cible peut déchiffrer les données password2.

Passage à une version antérieure d'une instance après la dépréciation de 3DES

Ce qui suit s'applique uniquement aux instances dont les champs password2 ont des longueurs d'entrée supérieures à 125 caractères et vous avez déjà déconseillé le chiffrement 3DES.

Pour passer à une version antérieure d'une instance afin qu'elle soit publiée plus tôt que Vancouver via le clonage d'instance, procédez comme suit avant de lancer le clone.

1. Vérifiez si la conservation des données est configurée pour préserver les données de champ password2.
2. Si oui, avant de demander un clone, contactez le ServiceNow support technique pour désactiver l'obsolescence de 3DES. Dans le champ **Motif** , utilisez « Cloner le passage à une version antérieure prérequis pour la prise en charge de password2 ».

Champs password2 hérités

Votre instance utilise le chiffrement 3DES pour convertir les données password2 en données héritées (pré-Rome) password2. Après avoir déconseillé le chiffrement 3DES, cette option n'est plus disponible. Si vous avez toujours besoin de cette fonctionnalité, demandez une dépréciation partielle (voir les détails dans la section suivante).

Comment déconseiller 3DES

Une fois que vous avez examiné les cas d'utilisation précédents, utilisez l'article de la base de connaissances KB1704481, pour un processus étape par étape visant à déconseiller en toute sécurité l'utilisation de l'algorithme DES ou Triple DES dans l'instance. Pour plus de détails, voir KB1704481 .

Important :
Vous devez vous élever au rang d'administrateur de sécurité pour voir le module **Conformité de sécurité** et effectuer ces étapes. Pour obtenir plus de détails sur ce processus, voir Accéder à un rôle privilégié.

Après la dépréciation de GlideEncrypter

Une fois le processus de dépréciation terminé, les informations suivantes s'appliquent à votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les champs password2 prennent toujours en charge le déchiffrement (mais pas le chiffrement) des données chiffrées 3DES.
- Les données chiffrées 3DES existantes dans les champs password2 restent telles quelles jusqu'à ce que la valeur du champ soit mise à jour par un utilisateur ou un workflow.
- Toute mise à jour de la valeur d'un champ password2 supprime le texte chiffré 3DES et le remplace par le texte chiffré à l'aide KMF d'AES.
- Dans certaines situations, votre instance peut afficher une erreur lors de l'enregistrement des données de mot de passe :

  Action abandonnée : la valeur du mot de passe ne peut pas être enregistrée en raison d'un problème technique. Veuillez consulter KB1296997 pour obtenir de l'aide.

  Si cette erreur s'affiche, consultez les informations d'assistance dans l'article de la base de connaissances KB1296997 .

Échange de ressources du cadre de travail de gestion des clés

ServiceNow® Resource Exchange est une KMF fonctionnalité qui vous permet d'échanger des ressources entre les instances de manière sécurisée.

Terminologie

Lorsque vous utilisez le Resource Exchange, faites référence à la terminologie suivante :

Resource Exchange Terminologie

Nom	Description
Resource Exchange	Processus d'échange de ressources entre les instances.
Key Exchange (KE)	Processus d'échange de clés sur des instances.
Instance de source de clé (source de clé)	L'instance propriétaire des clés.
Instance de cible clé (cible clé)	L'instance qui demande les clés.

Vue d'ensemble

Resource Exchange utilise les API cryptographiques pour assurer la confidentialité, l'intégrité, l'authentification KMF et la non-répudiation. Actuellement, Resource Exchange prend en charge la Key Exchange fonctionnalité. Consultez Cadre de travail de gestion de clés Échange de clés pour plus d'informations.

Cadre de travail de gestion de clés Échange de clés

KMF Key Exchange est une fonction de sous-ensemble de KMF Resource Exchange. Key Exchange transfère en toute sécurité des données chiffrées entre plusieurs instances.

Vue d'ensemble de Key Exchange

Key Exchange Transfère les clés en toute sécurité entre les instances.

KMF Key Exchange offre aux clients un moyen sécurisé d'échanger KMF des clés entre les instances. Le processus de clonage de données est un cas d'utilisation de l'application. Avec Key Exchange, les clés du module de chiffrement sont copiées lors du clonage des données des KMF composants. Les modules de chiffrement, les spécifications de clé de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

module et les politiques d'accès au module sont inclus dans le processus de clonage. Le transfert des clés n'est pas inclus.

Cette fonctionnalité est incluse dans le Cadre de travail de gestion des clés, qui est inclus dans le lot d'abonnement ServiceNow AI Platform Encryption. Pour en savoir plus sur ce produit, reportez-vous à la section Key Management Framework.

Utiliser Key Exchange

Les administrateurs qui utilisent KMF pour Chiffrement de champ peuvent cloner Key Exchange les clés entre les instances de production lors du clonage de données. Dans le clonage des données, l'administrateur/ KMF responsable cryptographique peut effectuer les opérations suivantes :

- Échanger toutes les clés vers les autres instances.
- Échangez des clés particulières une fois ou périodiquement avec l'autre instance.
- Envoyez des demandes à la demande à partir de l'instance cible vers l'instance source clé.
- Échangez les clés de la source vers la cible pour une nouvelle saisie du texte chiffré.
  - Gérez le délai d'expiration de la demande avec la possibilité de supprimer les clés ou de rejeter la demande d'échange de clé si la demande a expiré.
  - Une fois la demande terminée et la clé importée, la clé utilisée sera définie comme expirée et horodatage.
  - Retapez le texte chiffré sur l'instance cible qui a été chiffré avec les clés de la source.

Modes pris en charge

Key Exchange Prend en charge plusieurs modes au niveau de spécification de chiffrement du module de chiffrement :

Mode	Description
Automatique (aucune configuration, comportement par défaut)	Toutes les clés sont envoyées automatiquement pendant le processus de clonage des données sans configuration supplémentaire.
Configurable (configuration unique)	L'administrateur configure les clés à envoyer pendant le processus de clonage des données.
Manuel (personne dans la boucle)	L'administrateur envoie une demande à la demande sur l'instance cible à la source. La demande doit être approuvée par un administrateur de l'instance source de clé.
Renouvellement de saisie (demande automatisée)	L'administrateur sélectionne l'option de renouvellement de saisie pendant le processus de configuration du clonage.

Configurer l'échange de clés

Cadre de travail de gestion des clés (KMF) génère des demandes d'échange de clé automatique pour les modules de chiffrement pris en charge lors de la nouvelle installation ou de la mise à niveau de l'instance. gère la clé de chiffrement des données localement pour l'instance.

Avant de commencer

Un module cryptographique avec une clé doit être créé dans les instances cible et source avant d'être utilisé Key Exchange.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Key Exchange Les demandes sont lancées à partir de l'instance cible.

L'échange de clés automatique est actif par défaut lors du clonage d'une instance, où la propriété est clonée vers l'instance cible. En outre KMF, configurez les propriétés système pour gérer la façon dont les clés sont traitées lors d'un clone d'instance :

- **Désactiver l'échange de clés automatique :** Définissez la propriété sur **faux** pour les `glide_encryption.auto_key_exchange.enabled` demandes de clone récurrentes.
- **Envoyer des demandes d'échange de clé automatique** : définissez cette propriété sur **vrai**.

Important :
La propriété système de base est définie sur **true** par défaut, ce qui signifie que l'échange de clés automatique est activé lors du clonage d'une instance. Cette valeur doit être définie sur **faux** si vous utilisez la Renouvellement de saisie texte chiffré avec échange de clés fonctionnalité ou la fonctionnalité récurrente d'échange de clés. Consultez la rubrique Procédure pas à pas récurrente d'échange de clés pour en savoir plus.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Demandes d'échange de ressources** > **Nouveau**.
2. Remplissez les champs du formulaire.

Resource Exchange Champs du formulaire de demande

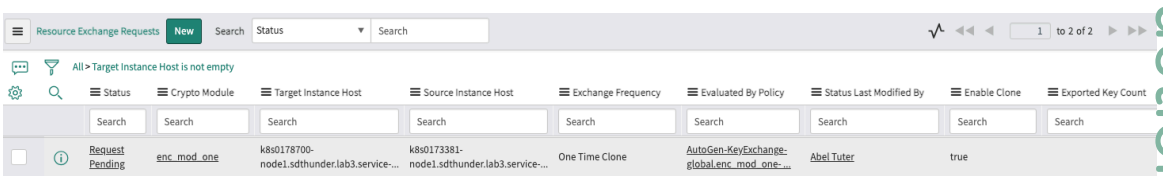
Nom	Description
Fréquence d'échange	○ **Adhoc** : envoie des demandes de l'instance cible clé à l'instance source. Entrez le sys_id d'instance et les informations sur l'hôte pour la source. Non pris en charge avec la nouvelle saisie de l'échange de clés. ○ **Clone unique** : échange unique des clés des spécifications de chiffrement source vers l'instance cible. ○ **Clone récurrent** : échangez les clés des spécifications de chiffrement source sélectionnées vers l'instance cible sur un clone récurrent défini.
<Source or Target> sys_id d'instance	○ **Adhoc** : saisissez la sys_id de l'instance source à laquelle vous souhaitez demander les clés. ○ **Clone unique**, **clone récurrent** : entrez le sys_id de l'instance cible qui envoie les demandes. **Conseil :** Entrez `stats.do` dans le navigateur d'application pour localiser l'ID de l'instance.
<Source or Target> Hôte d'instance	Entrez l'emplacement hôte ou le nom de l'instance source ou cible. **Conseil :** Par exemple, `instanceA.service-now.com`
Spécifications de chiffrement	Les clés de la spécification de chiffrement dans un module de chiffrement définissent les clés à cloner. Pour les demandes de clone ponctuelles et récurrentes, votre instance crée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

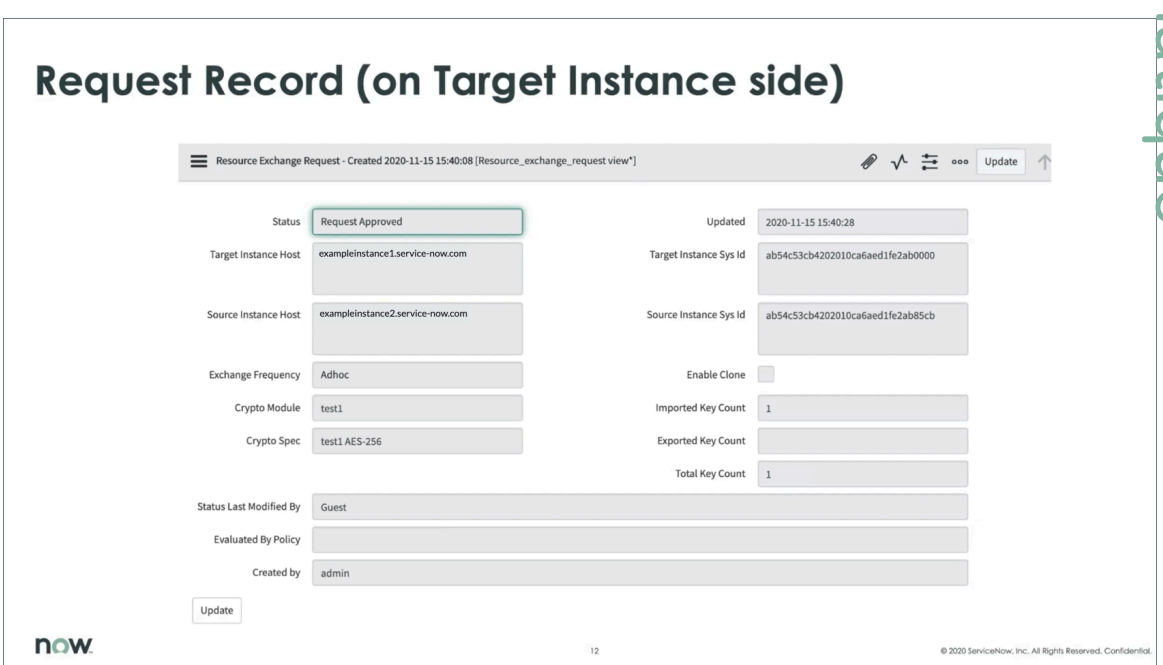
Nom	Description
	automatiquement une politique d’accès au module **d’échange de ressources** . Vous n’avez pas besoin de configurer une politique manuellement. **Remarque :** Sélectionnez l’icône Rechercher à l’aide d’une liste (icône pour parcourir les spécifications cryptographiques disponibles.
Activer le renouvellement de saisie après l’importation de la clé	Option permettant d’activer le renouvellement de saisie automatique.

3. Sélectionnez **Soumettre**.
   En cas de réussite, une confirmation s’affiche en haut du formulaire. La table Demandes est mise à jour avec l’entrée **Demande en attente** dans l’instance source et dans l’instance cible. Ouvrez l’enregistrement de la demande pour afficher l’état de la demande, le nombre de clés importées et le nombre total de clés sur la cible ou l’hôte source.



4. La demande en attente est acceptée dans l’instance source pour terminer l’échange.

   Au moment du clonage, la politique d’accès au module sur l’instance source est invoquée pour approuver automatiquement la demande et envoyer les clés à la cible nouvellement clonée.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Après une tentative d'échange de clé, votre instance de non-production met à jour la `protected.script.values.kmf.rekeyed` propriété système. Cette propriété est visible dans la table Propriétés système [sys_properties] après une tentative d'échange de clé. Si le chiffrement à l'aide de la clé échangée réussit, cette propriété a la valeur **vrai**. Sinon, la propriété a la valeur **faux**. Si la valeur est fausse, l'instance tente à nouveau de chiffrer le lendemain.

Renouvellement de saisie texte chiffré avec échange de clés

Resource Exchange Prend en charge la nouvelle saisie du texte chiffré sur l'instance cible qui a été chiffrée avec les clés de la source. L'activité de renouvellement de saisie est suivie dans le cycle de vie de la clé.

Vue d'ensemble

Les administrateurs qui utilisent KMF for Chiffrement de champ peuvent utiliser Key Exchange pour retaper des clés cryptographiques entre des instances de production lors du clonage de données. Une clé active doit d'abord être disponible sur l'instance cible pour renouvellement de saisie, car le renouvellement de saisie nécessite une clé active. Une tâche de chiffrement est automatiquement créée et exécutée par le système pour faire pivoter et ressaisir la clé source et chiffrer à nouveau le texte chiffré.

Utilisez Key Exchange pour effectuer les actions suivantes :

- Définissez un délai d'expiration pour le renouvellement de saisie.

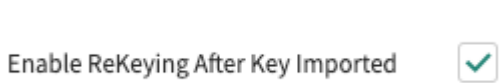
  Si la demande a expiré, la demande est rejetée et la clé est supprimée.

- Automatisez la nouvelle saisie du texte chiffré qui a été chiffré avec des clés provenant des instances sources.

  Une nouvelle clé de chiffrement clonée est utilisée pour chiffrer à nouveau le texte chiffré sur l'instance cible.

- L'objectif de renouvellement de saisie est défini pendant le processus de clonage et est automatisé dans le cadre du clone.
- Le suivi de l'activité de renouvellement de saisie est effectué dans l'onglet **Clé des modules** du module de chiffrement. Accédez à l'état du cycle de vie de la clé et à la version de la clé pour l'activité de la clé. Consultez Faire pivoter les clés pour plus d'informations.

Configurez un Key Exchange et cochez la case **Activer le renouvellement de saisie après l'importation de la clé pour** l'activer. Consultez Configurer l'échange de clés pour en savoir plus.



Procédure pas à pas récurrente d'échange de clés

Cette procédure pas à pas permet de configurer un échange de clés récurrent dans votre instance à l'aide de and Resource Exchange.

Avant de commencer
Rôles requis : sn_kmf.cryptographic_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Cet exemple vous montre comment une instance cible demande des clés à une instance hôte.

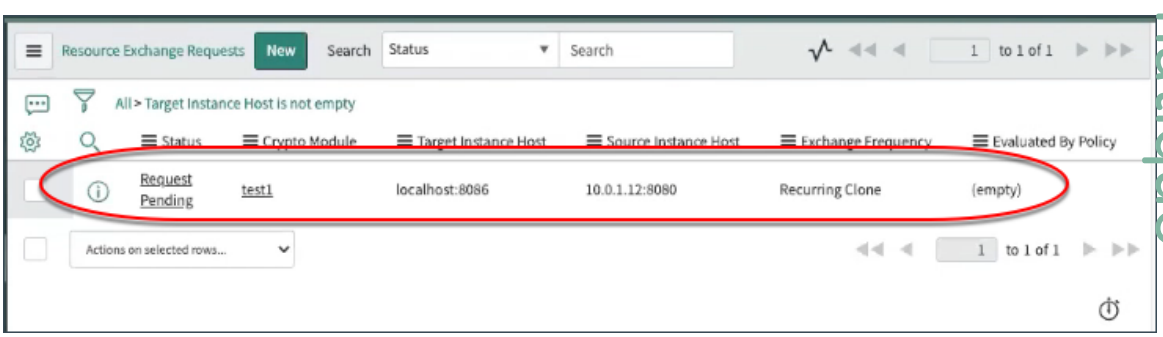
- Avant de pouvoir effectuer cette procédure, vous devez cloner une instance. Voir Clone système pour plus d'informations.
- **Échange de clés automatique** : la propriété *glide_encryption.auto_key_exchange.enabled* système de base est **true** par défaut, ce qui signifie que l'option automatique est activée lors du clonage d'une instance. La propriété est clonée sur l'instance cible.
- Désactivez l'automatique en définissant la propriété sur **faux**.

Procédure

1. Sur l'instance source, créez un module de chiffrement ou accédez à un module de chiffrement existant à l'aide de column_level_encryption et configurez les configurations de champs chiffrés pour le chiffrement de texte chiffré pour Key Exchange.
   Voir et pour plus de détails.
   a. Assurez-vous que les clés ont été générées dans le module de chiffrement.

   Remarque :
   Votre instance crée automatiquement une politique d'accès au module lors de l'exécution de la demande de clone.

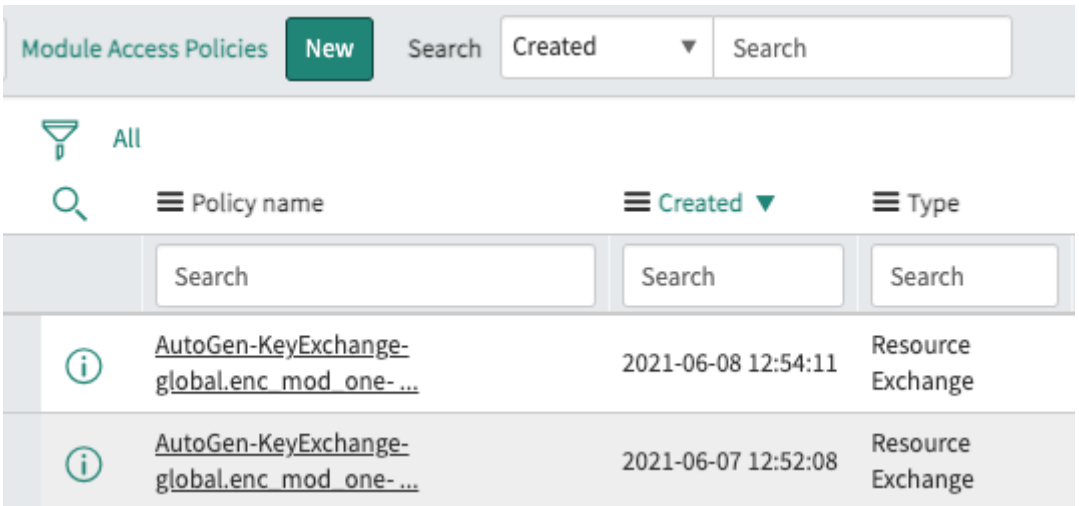
2. Depuis l'instance clonée, accédez à **Gestion des clés** > **Demandes d'échange de ressources** > **Nouveau**.
3. Remplissez le formulaire et sélectionnez **Clone récurrent** comme fréquence d'échange.
4. Depuis l'instance cible du clone, accédez à **Gestion des clés** > **Demandes d'échange de ressources**.
   La demande de l'instance hôte s'affiche dans la table.



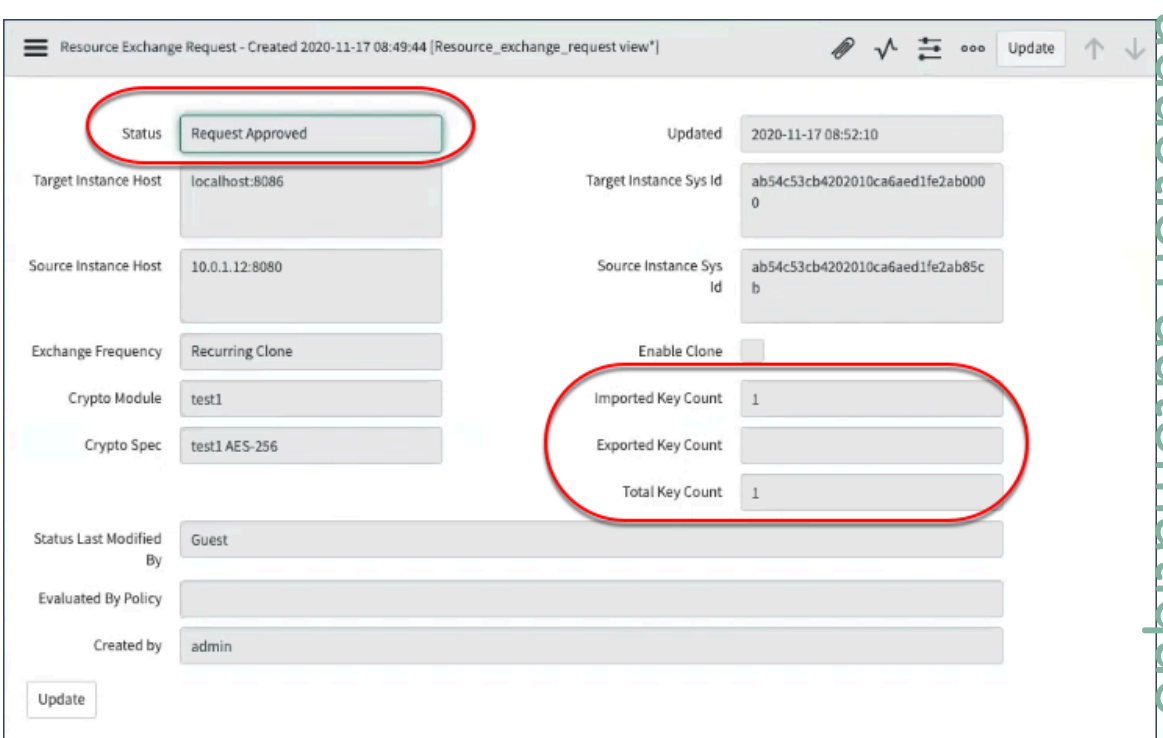
Important :
Pour les demandes de clone ponctuelles et récurrentes, votre instance crée automatiquement une politique d'accès au module. Vous n'avez pas besoin de configurer une politique manuellement. Au moment du clonage, cette politique sur l'instance source est invoquée pour approuver automatiquement la demande et envoyer les clés à la cible nouvellement clonée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



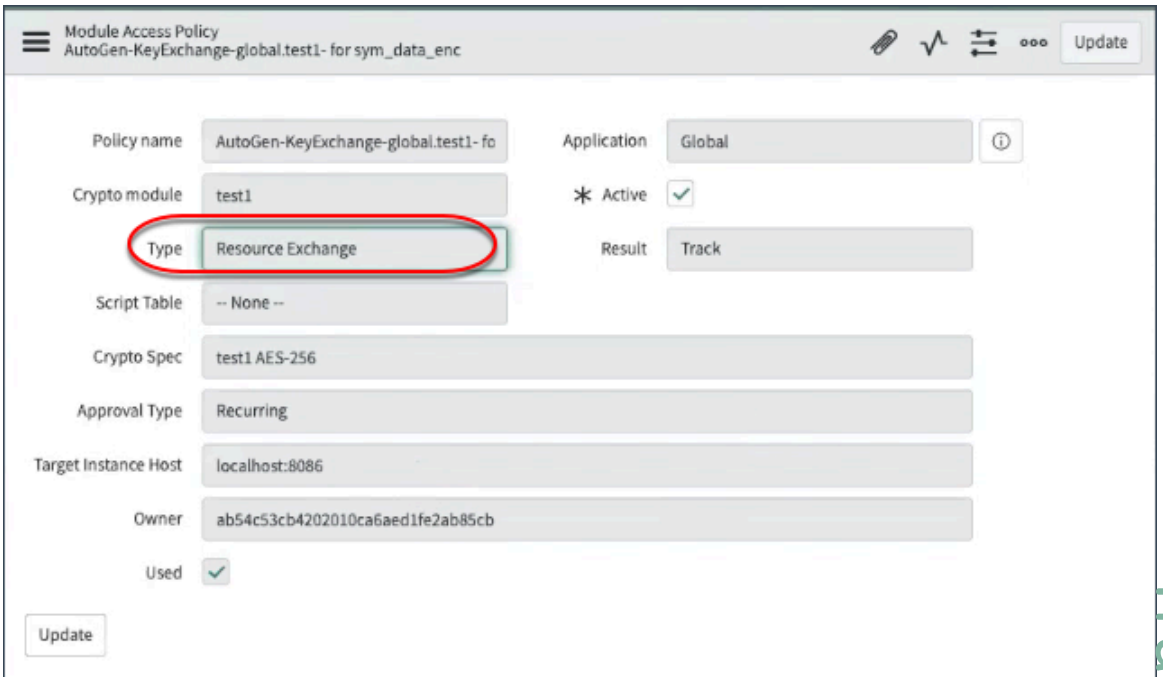
Dans le formulaire Demandes, l'état est mis à jour sur **Demande approuvée** et le champ **Nombre de clés importées** apparaît sur l'enregistrement.



Traduction automatique

5. Retournez à l'instance hôte.
6. Affichez l'enregistrement de la demande pour voir le nombre de clés exportées.
7. Affichez l'enregistrement de la politique d'accès au module pour voir que le **type** est Resource Exchange.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Resource Exchange prend également en charge la nouvelle saisie du texte chiffré sur l'instance cible. Consultez la section pour en savoir plus.

Résultats
Après une tentative d'échange de clé, votre instance de non-production met à jour la `protected.script.values.kmf.rekeyed` propriété système. Cette propriété est visible dans la table Propriétés système [sys_properties]. Si le chiffrement à l'aide de la clé échangée réussit, cette propriété a la valeur **vrai**. Sinon, la propriété a la valeur **faux**. Si la valeur est faux, votre instance essaiera de chiffrer à nouveau le lendemain.

Sécurité de l'infrastructure

Utilisez les outils de sécurité de l'infrastructure pour créer, charger et gérer les certificats que votre instance utilise pour chiffrer le trafic du client au serveur.

Le module d'extension Infrastructure Security fournit les outils que vous pouvez utiliser pour gérer les chiffrements et les certificats TLS (Transport Layer Security). Votre instance utilise TLS pour chiffrer le trafic du client vers votre serveur.

Sélectionner les chiffrements utilisés sur votre instance

À l'aide de la **page TLS**, les administrateurs peuvent configurer les chiffrements de centre de données à utiliser sur leur instance, ainsi que sélectionner l'ordre dans lequel les chiffrements sont essayés.

Générer et charger vos propres certificats

Utilisez les outils de sécurité de l'infrastructure pour générer vos propres demandes de signature de certificat, qui peuvent être signées par l'autorité de certification de votre choix. Ensuite, vous pouvez utiliser les outils pour charger le certificat signé sur l'équilibreur de charge de votre instance.

Surveiller l'état de vos chiffrements et certificats

Utilisez les pages **Paramètres TLS** et **Paramètres SYOC** pour afficher l'état des modifications que vous avez apportées à vos chiffrements et certificats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer le module d'extension Sécurité de l'infrastructure

Installez le module d'extension Paramètres de sécurité d'infrastructure ServiceNow (com.glide.infrastructure_security) pour commencer à utiliser ces fonctionnalités. Pour en savoir plus sur l'activation d'un module d'extension, consultez Activer un module d'extension .

Après avoir installé le module d'extension, activez la fonctionnalité Signer votre propre sécurité (SYOC) en définissant la *sn_infra_sec.syoc.enabled* propriété système sur vrai.

Remarque :
Si la *sn_infra_sec.syoc.enabled* propriété n'est pas disponible sur votre instance, vous devez la créer. Pour obtenir des détails sur ce processus, consultez Add a system property .

Générer une demande de signature de certificat

Utilisez la page Générer une signature de certificat (CSR) pour créer une demande de signature de certificat afin de prendre en charge les certificats signés par le client pour votre équilibreur de charge d'instance.

Avant de commencer

Rôle requis : admin

Le module d'extension Sécurité de l'infrastructure (com.glide.infrastructure_security) doit être installé pour effectuer ces étapes. Consultez la sectionSécurité de l'infrastructure pour en savoir plus sur ce module d'extension.

Pour plus d'informations sur l'utilisation d'URL personnalisées avec ServiceNow, reportez-vous à la section Définir une URL personnalisée comme URL d'instance.

Procédure

1. Accédez à la **Tous** > **Paramètres de sécurité de l'infrastructure** > **Générer un CSR**.
2. Ajoutez un ou plusieurs domaines à votre demande.
   a. Sélectionnez le bouton **Ajouter** sous l'en-tête **Domaines** .
   b. Dans la fenêtre contextuelle, saisissez le domaine et sélectionnez **OK**.
   c. Répétez ces étapes si nécessaire pour ajouter d'autres domaines.

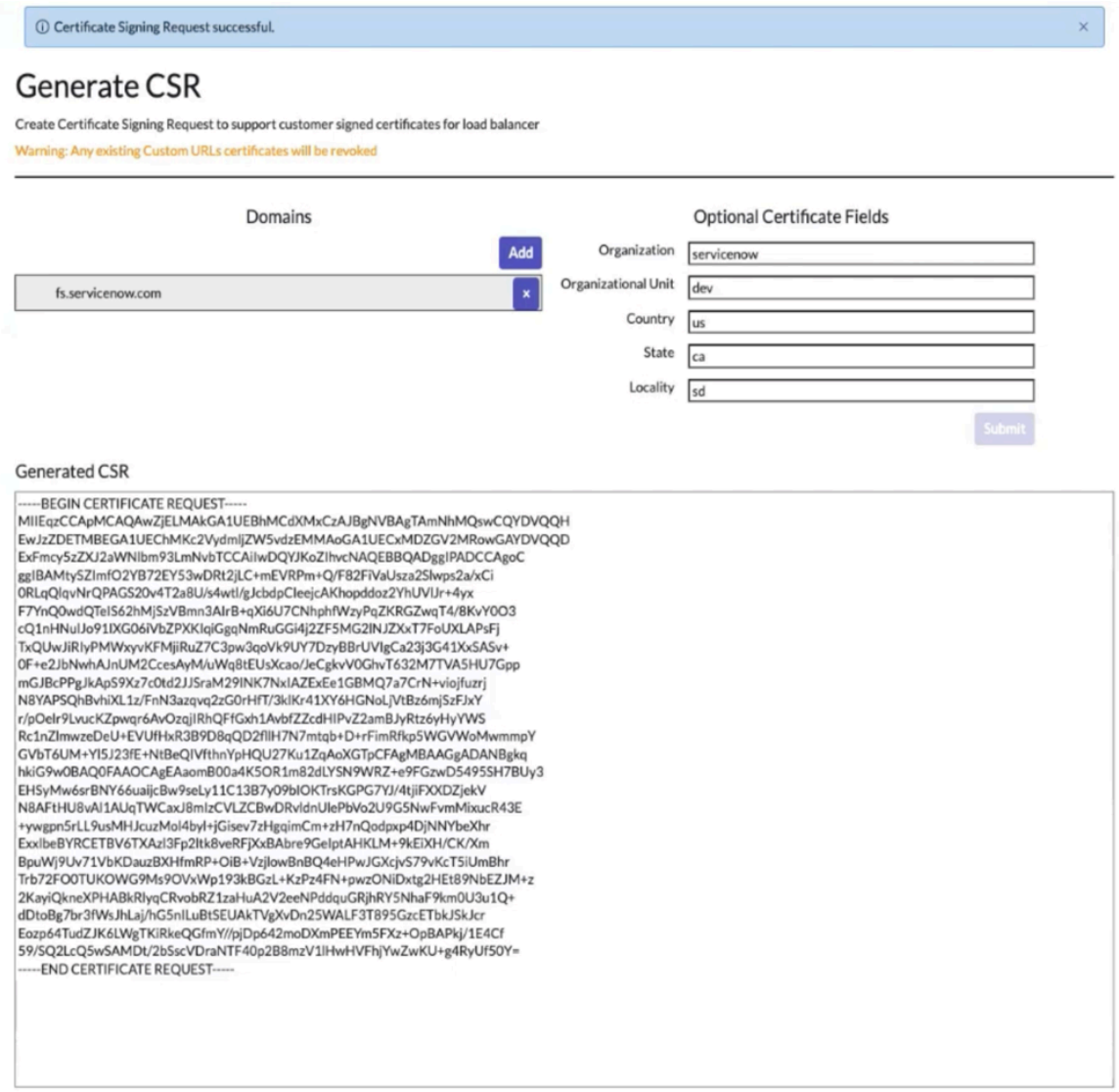
   Remarque :
   Les domaines peuvent être supprimés en sélectionnant le bouton X à gauche de chaque entrée de domaine.
3. Saisissez toutes les informations que vous souhaitez inclure dans votre demande dans les **champs de certificat facultatifs**.
4. Sélectionnez **Soumettre**.

Avertissement :
Vous ne pouvez pas soumettre une demande alors qu'une autre demande est en cours de génération. Si ce problème se produit, une erreur « Ressource en conflit » s'affiche. Pour la traiter, annulez la demande actuelle ou attendez le traitement de la demande actuelle avant d'en soumettre une autre.

Après **avoir sélectionné Soumettre**, votre instance génère la demande de signature de certificat. La demande s'affiche dans le champ **CSR généré** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Copiez le contenu du champ **CSR généré** .

Chiffrement Password2 avec Key Management Framework (KMF)

Pris en charge par , utilisez le type de champ (chiffré dans les Cadre de travail de gestion des clés deux sens) pour chiffrer et déchiffrer les Password2 champs personnalisés avec la séparation des tâches, la protection des clés et la gestion du cycle de vie. Il fonctionne conformément aux directives NIST 800-57 et offre une protection FIPS 140-2-L3.

Password2 est un champ de texte qui stocke les mots de passe avec un chiffrement bidirectionnel. Le chiffrement bidirectionnel stocke les mots de passe sous la forme d'une valeur chiffrée sécurisée qui peut être déchiffrée au sein de l'instance.

Conseil :
À partir de la version, les Vancouver administrateurs peuvent déconseiller le chiffrement 3DES sur les champs password2 en faveur du nouveau AES (Advanced Encryption Standard). Pour plus de détails, voir Déconseiller l'utilisation de GlideEncrypter de 3DES pour les champs password2.

Activation

Password2 La fonctionnalité est active par défaut. Il est contrôlé par la `glide.kmf.encrypter.enabled` propriété, qui est définie sur **vrai** pour toutes les

Traduction automatique

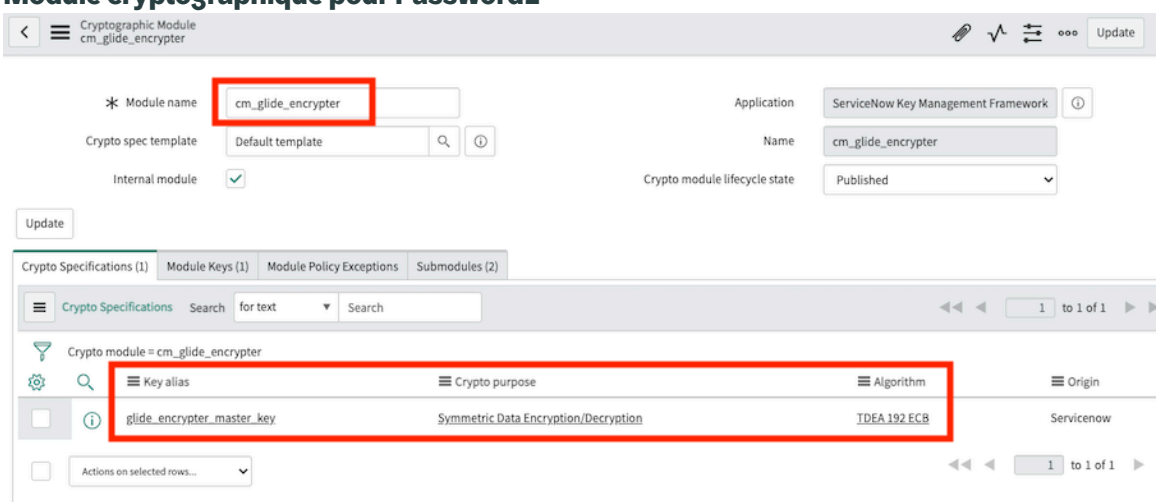
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nouvelles instances et mises à niveau. Vous n'avez pas besoin d'activer Chiffrement de champ Enterprise pour utiliser Password2.

Mode de fonctionnement de Password2

Le Cadre de travail de gestion des clés fournit un module cryptographique parent du système de base **cm_glide_encrypter**. Ce module fournit une spécification cryptographique et une clé permettant de déchiffrer les champs hérités Password2 .

Module cryptographique pour Password2



Ce module cm_glide_encrypter peut avoir des sous-modules, chacun ayant sa propre clé de module et spécification. Si un sous-module est présent avec le même périmètre d'application que l'application où se trouve le Password2 champ, le système utilise le sous-module. Par exemple, si une table de l'application ServiceNow® Service client comporte un sous-module et que vous écrivez des informations dans un Password2 champ d'une table du périmètre de l'application Service client , le processus cryptographique appelle le Service client sous-module. Le processus utilise également la clé de ce sous-module pour le chiffrement et le déchiffrement avec une clé de chiffrement AES 256 GCM unique. Un sous-module par périmètre de l'application est autorisé. Le module parent n'est pas toujours utilisé pour le champ d'application global. Généralement, les nouveaux champs utilisent instance_level_glide_encrypter.

Remarque :
Vous ne pouvez pas créer vos propres sous-modules dans Yokohama. Des sous-modules sont fournis dans divers modules d'extension d'application sur le ServiceNow AI Platform. Vous pouvez faire pivoter les clés sur les sous-modules, mais pas sur le module cm_glide_encrypter parent.

Séparation de domaine et clients sur site

KMF Password2 ne prend pas en charge Séparation de domaine. Vous pouvez l'utiliser Password2 avec des instances sur site.

Hérité Password2 et actuel Password2

Dans Yokohama, le champ existant Password2 a été mis à niveau.

L'implémentation actuelle de Password2:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilise les directives d'encapsulation de clé conformément à la Cadre de travail de gestion des clésnorme NIST 800-57 et fournit une protection FIPS 140-2-L3 pour l'ensemble de la hiérarchie de clés.
- Inclut des options pour créer des sous-modules dédiés et uniques KMF Password2 pour des applications spécifiques, offrant un contrôle via le périmètre de l'application. Chaque sous-module possède sa propre clé de chiffrement AES 256 GCM.

Champs Password2 dans les scripts

Lorsque vous accédez à Password2 des champs avec un script, exécutez le script dans le même champ d'application que le champ d'application de la table. Utilisez setDisplayValue() pour chiffrer Password2 les valeurs et getDecryptedValue() pour déchiffrer et lire la valeur.

Remarque :
N'utilisez pas l'API GlideEncrypter() sur Password2 les champs.

Cet exemple de script vous montre comment chiffrer my@Password dans la colonne password2 de la table 'table_xyz'.

```
var  gr =  new GlideRecord('table_xyz');
gr.pwd2column_name.setDisplayValue('my@Password');

gr.insert();
```

Important :
Vous ne pouvez pas utiliser l'API setValue() pour le Password2 champ.

Cet exemple de script vous montre comment déchiffrer le même champ pour récupérer la valeur :

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Important :
L'API getDecryptedValue() n'est pas incluse dans le périmètre. Il est disponible dans le monde entier.

1. Lorsque vous chiffrez des données dans un Password2 champ, le système détermine le périmètre de l'application où se trouve le Password2 champ.
2. Le système recherche alors un sous-module du module parent **cm_glide_encrypter** ayant le même périmètre que l'application si la propriété est définie sur *true*.

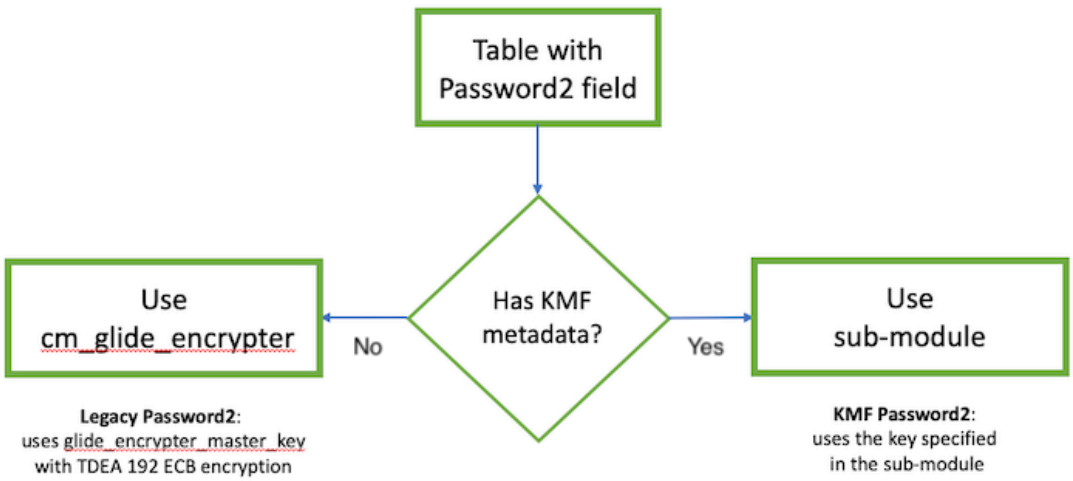
   Remarque :
   Si un sous-module avec le même champ d'application est présent, il utilise la spécification et la clé du sous-module pour effectuer le chiffrement.

Cette illustration explique comment votre instance déchiffre les données dans Password2 les champs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de déchiffrement Password2



KMF Password2 Tâche de migration

Une tâche de migration est fournie pour les clients effectuant une mise à niveau à partir de versions précédentes. Il prend des données chiffrées avec un chiffrement hérité Password2 et les chiffre à nouveau avec la clé d'une KMF Password2 clé de sous-module. Le rechiffrement s'applique uniquement aux tables avec Password2 des champs dans les périmètres d'application qui ont également des sous-modules créés pour ce périmètre. Par exemple, un champ hérité Password2 dans **XYZ_example** application (avec **XYZ_example** périmètre de l'application) est chiffré à nouveau uniquement si un sous-module pour le périmètre de l'application **XYZ_example** existe sous le module parent cm_glide_encrypter.

Les KMF Password2 clés de chiffrement du sous-module sont protégées (chiffrées par enveloppe) dans la hiérarchie des KMF clés.

Certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les principales caractéristiques et la valeur commerciale des certificats.

Configurer



Planifiez vos configurations de base.

Charger



Planifiez et configurez l’application.

Traduction automatique

Explorer les certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les certificats sont utilisés pour des fonctionnalités telles que :

- LDAPS
- Outbound web service mutual authentication
- Sécurité des services Web
- MID Server

Pour utiliser un certificat, vous devez générer ou acheter un certificat pour le serveur sécurisé ou le client et le charger sur une instance.

Certificats LDAP

Un certificat SSL est requis pour que l'instance établisse une connexion LDAP sur SSL (protocole LDAPS) avec un serveur LDAP.

L'instance accepte deux types de certificats LDAP :

Certificat	Type	Requis pour
Certificat du serveur LDAP	Tout type pris en charge	Toutes les configurations LDAP
Certificat client LDAP	Type de keystore Java	Authentification réciproque

S'il existe plusieurs certificats de serveur, l'instance essaie chaque certificat de serveur à tour de rôle jusqu'à ce que le serveur LDAP autorise la connexion. Si vous utilisez plusieurs serveurs LDAP, assurez-vous d'inclure le certificat SSL de chaque serveur LDAP.

L'authentification réciproque nécessite que le client présente un certificat en plus du serveur. Si votre serveur LDAP nécessite l'authentification réciproque, vous devez également fournir le certificat client de votre serveur LDAP dans un certificat de type de magasin de clés Java.

Critères de certification

Un certificat valide doit répondre à ces critères :

- Le certificat peut avoir une taille de clé allant jusqu'à 2 048 bits.
- Le certificat doit avoir l'une de ces extensions de fichier :

Extension	Description
DER	Le format *Distinguished Encoding Rules* est une syntaxe de transfert de message binaire. Ce format prend également en charge le format . CER et . Extensions de fichiers CRT.
CER	Extensions de fichier de certificat pour les certificats utilisant le format de règles de codage distinguées.
Tube cathodique	Extensions de fichier de certificat pour les certificats utilisant le format de règles de codage distinguées.
PEM	Le format Privacy *Enhanced Mail* est un certificat DER codé en base 64 entre les chaînes de texte « -----BEGIN CERTIFICATE----- » et « -----END CERTIFICATE-----« .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Certificat de confiance

Par défaut, votre instance ne fait confiance qu'aux certificats d'une autorité de certification (CA) reconnue dans la Java Virtual Machine (JVM). Les certificats auto-signés et signés par l'entreprise ne sont pas approuvés.

Remarque :
Pour en savoir plus sur les propriétés qui affectent l'utilisation des certificats, consultez Paramètres de renforcement de la sécurité de l'instance.

Génération d'un certificat client LDAP

Générez un certificat client LDAP pour l'authentification réciproque à l'aide d'OpenSSL. La sortie finale est un certificat PKCS#12 stocké dans un magasin de clés Java.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Consultez la documentation OpenSSL pour plus d'informations sur la génération de certificats. Ces étapes supposent que vous avez accès à OpenSSL.

Entrez ces commandes dans une interface de ligne de commande.

Procédure

1. Générez un certificat client auto-signé.

   Example
   Par exemple, cette commande crée un certificat client test1-cert.crt basé sur la clé privée test1-key.key.

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out
    test1-cert.crt
   ```

2. Convertir le fichier de certificat et la clé privée en PKCS#12 (un fichier avec une extension .pfx ou .p12).

   Example
   Par exemple, cette commande convertit le certificat client et la clé privée en un certificat PKCS#12 appelé test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Générez le magasin de clés Java et importez-y le fichier pkcs12.

   Example
   Par exemple, cette commande importe le certificat dans le magasin de clés Java test1.jks.

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12
    -destkeystore test1.jks
   ```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Chargez le certificat dans le fichier du magasin de clés (`test1.jks`) dans l'instance.

Remarque :

Si vous chargez vers une instance sur site à l'aide d'un certificat avec l'extension .jks et que vous recevez une erreur indiquant « Aucun certificat valide trouvé pour traiter le téléchargement de l'application », utilisez plutôt un certificat avec l'extension .pfx.

Que faire ensuite

Chargement d'un certificat sur une instance

Génération d'un certificat de serveur

Vous pouvez utiliser keytool pour générer un nouveau fichier de magasin de clés Java, créer une demande de signature de certificat (CSR) et importer la clé privée, la paire de certificats publics et les certificats signés dans le magasin de clés.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Consultez la documentation Java keytool pour plus d'informations sur la génération de clés et de CSR.

Entrez ces commandes dans une interface de ligne de commande :

Procédure

1. Générez un magasin de clés Java et une paire de clés.

Example

Par exemple, cette commande crée un magasin de clés appelé my.keystore et génère une clé privée appelée mydomain dans le magasin de clés.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Générez une CSR pour un magasin de clés Java existant.

Example

Par exemple, cette commande génère une CSR appelée mydomain.csr ou la clé mydomain.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importez un certificat *d'autorité de certification* racine ou intermédiaire, ou CA, dans le magasin de clés Java.

Example

Par exemple, cette commande importe le certificat de l'autorité de certification pour Thawte. Cette commande suppose que Thwate est l'autorité de certification qui a signé la CSR.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importez un certificat primaire signé dans le magasin de clés Java.

Example

Par exemple, cette commande importe le certificat signé mydomain.crt dans le magasin de clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

5. Chargez le certificat dans le fichier keystore (my.keystore) sur l'instance.

Que faire ensuite

Chargement d'un certificat sur une instance

Chargement d'un certificat sur une instance

Ajoutez un certificat à l'instance à partir du module Certificats.

Charger un certificat sur une instance

Chargez un certificat sur une instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lorsqu'un certificat est mis à jour sur le serveur ADFS, vous devez également charger un certificat mis à jour dans l'instance.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Certificats**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.
4. Sélectionnez **Soumettre**.

   Lors du chargement, le module extrait et affiche les propriétés en lecture seule du certificat dans les champs suivants :

   - Date de début de validité
   - Date d'expiration
   - Émetteur
   - Objet de la certification

5. Sélectionnez **Valider les banques/certificats** pour vérifier si le certificat est correct.
   Si l'instance rencontre des erreurs avec le certificat ou le magasin de clés, elle affiche un message d'erreur.

Chargement d'un certificat de serveur de confiance

En chargeant le certificat de serveur de confiance du fournisseur de service, l'instance s'assure qu'elle se connecte à un service valide et sécurisé.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'instance valide les appels de service Web sortants à l'aide du certificat fourni par le fournisseur de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez un enregistrement de certificat avec le type **Certificat de magasin de confiance**.
2. Effectuez l'une des actions suivantes :
   - Joindre le certificat au format DER du fournisseur de service.
   - Copiez et collez le certificat au format PEM du fournisseur de service dans le champ **Certificat PEM** .

Chiffrement de champ

Protégez les données chiffrées de votre instance contre les utilisateurs, scripts ou processus système non autorisés à l'aide de Chiffrement de champ.

Chiffrement de champ est un produit de chiffrement basé sur . ServiceNow Cadre de travail de gestion des clésChiffrement de champ permet le chiffrement de champs ou de pièces jointes spécifiques au sein d'une instance. À utiliser Chiffrement de champ en combinaison avec le chiffrement dans le cloud et les listes de contrôle d'accès (ACL) pour protéger les informations sensibles des utilisateurs connectés qui ne sont pas autorisés à les consulter.

Chiffrement de champ a deux versions disponibles.

Chiffrement de champ Démarreur

Chiffrement de champ Starter est inclus gratuitement sur la plateforme et prend en charge le ServiceNow chiffrement d'un nombre limité de champs.

Chiffrement de champ Enterprise

Chiffrement de champ Enterprise est une version premium avec abonnement du produit disponible pour les clients abonnés à ServiceNow Vault, Platform Encryption ou Chiffrement de champ Enterprise.

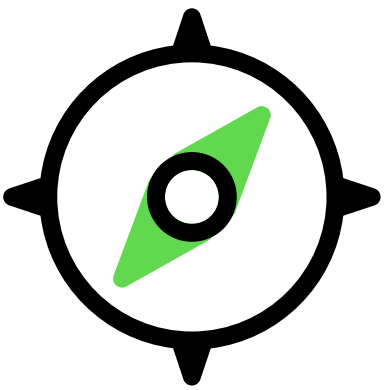
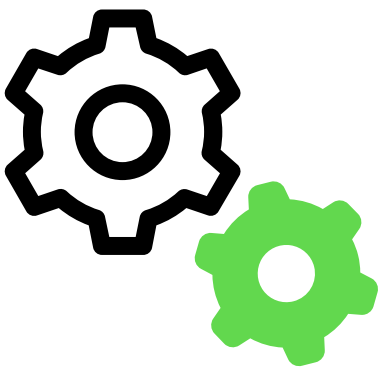
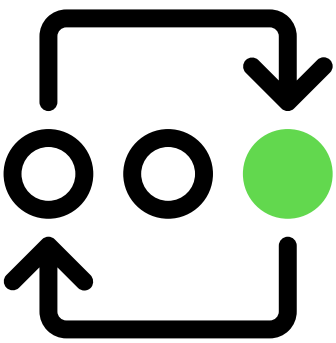
Pour plus d'informations sur la différence entre ces versions, reportez-vous à la section Explorer Chiffrement de champ.

Chiffrement de champ remplace le produit disponible dans les Chiffrement au niveau des colonnesXanadu versions antérieures et ultérieures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

Explorer	Configurer	Utiliser
		
Découvrez les avantages des versions Starter et Enterprise de Chiffrement de champ.	Découvrez comment activer, configurer Chiffrement de champ Enterprise et gérer la migration à partir de la prise en charge du chiffrement ou Chiffrement au niveau des colonnes.	Utilisez cette fonction Chiffrement de champ pour gérer l'accès aux données chiffrées sur vos instances

Ressources utiles

Voici quelques ServiceNow ressources qui peuvent vous fournir des informations utiles :

ServiceNow Community

Communauté ServiceNow

Centre de réussite client

Customer Success Center

Promoteur

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow University

NowCreate

Now Create

Partenaire

https://www.servicenow.com/partners.html

ServiceNow

https://www.servicenow.com/

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Store

https://store.servicenow.com/

Soutien

https://support.servicenow.com/now

Portail d'erreurs connues

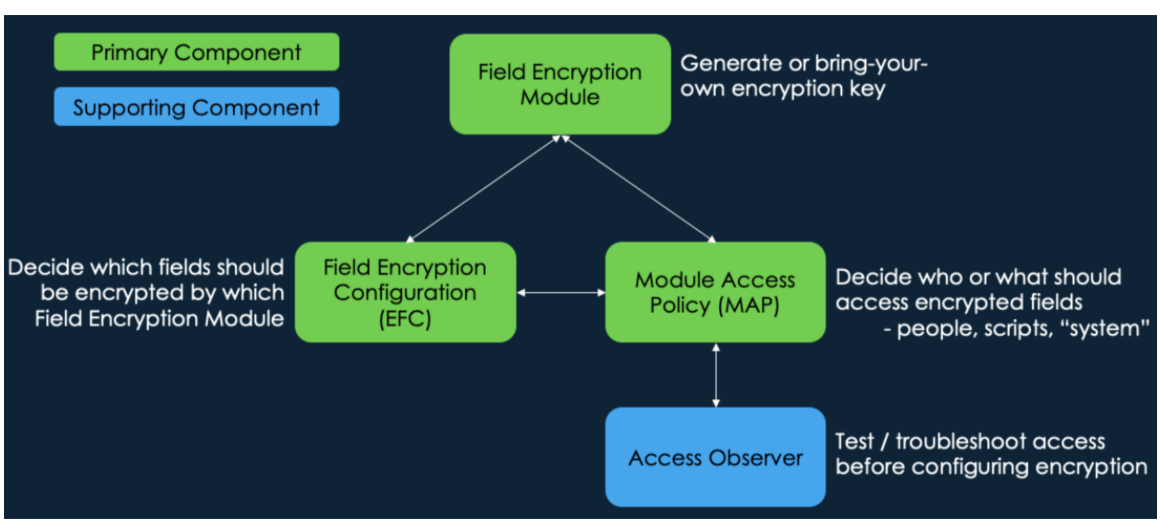
Explorer Chiffrement de champ

En savoir plus sur Chiffrement de champ Starter et Chiffrement de champ Enterprise

Contrôle d'accès crypté

Par défaut, Chiffrement de champ bloque tous les utilisateurs, scripts et processus système l'accès aux données chiffrées. Toutefois, Chiffrement de champ dispose d'une fonctionnalité de contrôle d'accès qui est utilisée en combinaison avec les listes de contrôle d'accès (ACL), mais également distincte de celles-ci pour garantir que seuls les utilisateurs, scripts ou processus système appropriés peuvent accéder aux données chiffrées.

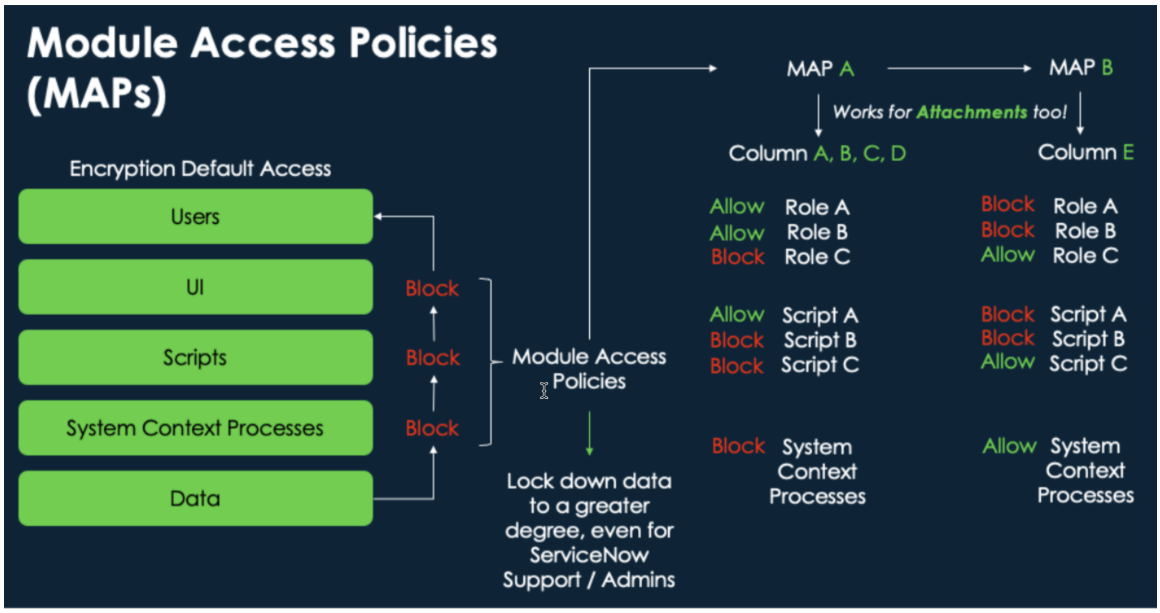
Vous pouvez configurer Chiffrement de champ la fonctionnalité de contrôle d'accès de via une combinaison de modules, de configurations de champs chiffrés et de politiques d'accès Chiffrement de champ aux modules. L'image suivante montre comment ces trois composants fonctionnent ensemble.



Les politiques d'accès au module (illustrées dans l'image suivante) permettent aux utilisateurs, aux scripts ou aux processus système d'accéder aux données chiffrées (mais par défaut, les données chiffrées sont verrouillées pour empêcher tout accès dans l'instance).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Différences entre Chiffrement de champ Starter et Chiffrement de champ Enterprise

L'ensemble des fonctionnalités est différent entre Chiffrement de champ Starter et Chiffrement de champ Enterprise.

Fonctionnalité	Chiffrement de champ Démarreur	Chiffrement de champ Enterprise
Nombre de champs chiffrés	Jusqu'à 5 champs chiffrés	Aucune restriction sur le nombre de champs chiffrés
Chiffrement de la pièce jointe	Non	Oui
Gestion des clés	Aucun (contactez ServiceNow le support pour la rotation des clés)	Gérer les clés de votre instance sans l'intervention de l'assistance ServiceNow
Types de données pris en charge	Tous les types de données pris en charge	Tous les types de données pris en charge
Nombre de modules de chiffrement de champ	Aucune restriction	Aucune restriction
Nombre de politiques d'accès au module	Aucune restriction	Aucune restriction

Chiffrement de champ utilisateurs

Utilisateurs

Utilisateur	Description
Cadre de travail de gestion des clés (KMF)Admin ou gestionnaire cryptographique KMF	Ces rôles sont utilisés pour configurer des éléments de Chiffrement de champ. • Chiffrement de champ Modules et clés de module • Spécifications cryptographiques • Politiques du cycle de vie des modules

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs (suite)

Utilisateur	Description
	• Configurations de champs chiffrés pour les champs et les pièces jointes • Politiques d'accès au module (MAP) • Configure, encapsule et charge les clés fournies par le client (pour Chiffrement de champ Enterprise) • Configure Access Observer et examine les journaux Access Observer. • Planifier le chiffrement, le déchiffrement ou la nouvelle saisie en masse
Opérateur de chiffrement KMF	Configure les propriétés des clés fournies par le client

Chiffrement de champ et l'historique des enregistrements

Les changements apportés aux champs chiffrés Chiffrement de champ ne sont pas suivis dans le flux d'activité de l'enregistrement ni dans la table Historique des enregistrements [sys_history_set].

Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de Chiffrement de champ, consultez :

- Configurer Chiffrement de champ
- Utiliser Chiffrement de champ

Configurer Chiffrement de champ

Découvrez comment activer, configurer Chiffrement de champ et gérer la migration à partir de la prise en charge du chiffrement.

Activer Chiffrement de champ

Découvrez comment activer l'un ou l'autre ou Chiffrement de champ Enterprise.

Rôles requis pour configurer le chiffrement de champ

Découvrez les rôles requis pour configurer Chiffrement de champ.

Migration à partir de la prise en charge du chiffrement

Utilisez les travaux planifiés pour migrer vos clés et données chiffrées de la prise en charge du chiffrement hérité vers Chiffrement de champ Enterprise. Pour plus de détails sur ce processus, consultez Migration vers Chiffrement de champ Enterprise

Modifier les paramètres de chiffrement de la pièce jointe

Améliorez la sécurité en empêchant les utilisateurs de joindre des fichiers non chiffrés. Pour plus de détails, voir Empêcher les utilisateurs de joindre des fichiers non chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer Chiffrement de champ

Activez Starter Chiffrement de champ ou Chiffrement de champ Enterprise.

Avant de commencer

Rôle requis : admin

ServiceNow a été remplacé Chiffrement au niveau des colonnes par le Chiffrement de champ début dans la Yokohama mise en production.

Dans la version, les Yokohama clients qui n'ont jamais utilisé Chiffrement au niveau des colonnes auparavant peuvent commencer à utiliser Chiffrement de champ Starter ou Chiffrement de champ Enterprise la nouvelle structure de droits.

Les clients qui utilisaient Chiffrement au niveau des colonnes dans les versions précédentes et qui souhaitent commencer à utiliser Chiffrement de champ disposent des options suivantes :

Chiffrement de champ Démarreur

Chiffrement au niveau des colonnes Les clients Starter peuvent installer Chiffrement de champ Starter sans avoir besoin d'une nouvelle implémentation. Chiffrement de champ Starter reprend la configuration existante et ajoute de nouvelles fonctionnalités de manière transparente.

> **Avertissement :**
> Il existe des différences de droit entre Chiffrement au niveau des colonnes Starter et Chiffrement de champ Starter. Avant d'installer Chiffrement de champ Starter, assurez-vous que votre configuration est conforme aux autorisations. Pour en savoir plus sur les autorisations pour Chiffrement de champ Starter, reportez-vous à la section Explorer Chiffrement de champ.

Chiffrement de champ Enterprise

Chiffrement au niveau des colonnes Les clients d'entreprise doivent collaborer avec les équipes de leur compte pour s'assurer qu'ils disposent de l'autorisation appropriée pour Chiffrement de champ Enterprise. Une fois que cela se produit, le module d'extension Chiffrement de champ Enterprise peut être installé dans leurs instances.

> **Important :**
> Chiffrement au niveau des colonnes Enterprise n'accorde pas automatiquement un droit à Chiffrement de champ Enterprise, car il s'agit d'un produit différent, mais de remplacement.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**
2. Sous **Rechercher vos applications et modules d'extension sous licence**, recherchez Chiffrement de champ.
   La recherche doit révéler le module d'extension. Si vous avez acheté un abonnement pour Chiffrement de champ Enterprise, vous pouvez également voir ce module d'extension disponible.

> **Important :**
> Pour activer Chiffrement de champ Enterprise, vous devez d'abord acheter un abonnement. Votre chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les instances de production et non-production de votre organisation, en général en quelques jours à peine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez ou Chiffrement de champ Enterprise, puis sélectionnez **Installer**.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Besoins du rôle pour Chiffrement de champ

Découvrez les rôles requis pour configurer Chiffrement de champ.

La gestion nécessite les rôles suivants. Puisque est basé sur le Cadre de travail de gestion des clés, il existe des rôles communs aux deux.

- Administrateur
- Administrateur de sécurité
- Administrateur KMF
- Gestionnaire de chiffrement KMF

Pour en savoir plus sur les détails relatifs aux rôles, reportez-vous à la rubrique Rôles installés avec Key Management Framework.

Administrateur et administrateur de sécurité

Les utilisateurs doivent avoir le rôle d'administrateur pour accéder au rôle d'administrateur de sécurité. Vous devez disposer du rôle d'administrateur de sécurité pour effectuer des tâches de sécurité élevée, telles que la configuration de champs chiffrés et la configuration d'Observateur d'accès.

Les administrateurs peuvent s'élever au rang d'administrateur de sécurité à l'aide de cette procédure.

1. Sélectionnez votre photo de profil en haut à droite de l'écran.
2. Dans le menu déroulant, sélectionnez **Élever le rôle**.
3. Sélectionnez **Administrateur de sécurité**.
4. Sélectionnez **Enregistrer**.

Administrateur KMF

Les utilisateurs disposant du rôle administrateur peuvent affecter des utilisateurs au rôle administrateur KMF à l'aide de ce processus :

1. Accédez à la **Tous** > **Sécurité de système** > **Administration de la gestion de clés**.
2. À partir de la liste **Utilisateurs disponibles** , déplacez un utilisateur qui a besoin du rôle d'administrateur KMF vers la liste **Utilisateurs sélectionnés** .
3. Sélectionnez **Enregistrer**.

> **Important :**
> Pour éviter les problèmes de sécurité, évitez d'accorder le rôle d'administrateur KMF à plusieurs utilisateurs. Évitez d'affecter ce rôle à des utilisateurs lorsque des rôles plus spécialisés sont disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestionnaire de chiffrement KMF

Les utilisateurs disposant du rôle de gestionnaire de chiffrement KMF peuvent créer et mettre à jour des opérations sur les modules de chiffrement et les politiques d'accès aux modules. Les gestionnaires cryptographiques KMF peuvent également effectuer la gestion des clés et les opérations de cycle de vie.

Utilisez le processus suivant pour affecter ce rôle à un utilisateur.

1. Accédez à la **Tous** > **Sécurité de système** > **Utilisateurs**.
2. Sélectionnez un utilisateur qui doit configurer Chiffrement de champ.
3. Dans la liste connexe **Rôles** , sélectionnez **Modifier**.
4. Recherchez le gestionnaire sn_kmf.cryptographic et ajoutez le rôle de l'utilisateur sélectionné.
5. Sélectionnez **Enregistrer**.

Configurer les Chiffrement de champ modules

Apprenez à configurer Chiffrement de champ des modules.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire de chiffrement KMF

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Modules de chiffrement de champ**.
2. Sélectionnez **Nouveau**.
3. Dans le formulaire Module, renseignez les champs comme indiqué ici.

Champ	Valeur
Nom du module	Choisissez un nom pour le module. Ce nom est référencé lors de l'exécution de scripts.
Modèle de spécification de chiffrement	Renseigné automatiquement avec **le modèle par défaut**. Ce modèle est utilisé pour créer le module de chiffrement qui contient des mappages de nombreux objectifs de chiffrement sur des spécifications cryptographiques et des algorithmes recommandés.
Application	Périmètre de l'application pour ce module. Ce champ est automatiquement rempli avec l'application actuelle.
Nom	Ce nom est généré automatiquement. Il s'agit du nom du module ajouté au nom du périmètre de l'application pour éviter tout conflit avec d'autres applications incluses dans le périmètre. Par exemple, si vous créez un module portant le nom my_crypto_module dans le périmètre de l'application global, le nom est enregistré en tant que global.my_crypto_module.
État du cycle de vie du module de chiffrement	Le terme « cycle de vie » fait référence à la création, à l'utilisation et à la désactivation d'un module cryptographique. Définissez cette valeur sur **Brouillon** initialement lors de la configuration. Définissez-le sur **Publié** pour une utilisation active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	Remarque : Le modèle par défaut est automatiquement défini sur **Publié**.
Module de chiffrement parent	Pour Chiffrement de champ, assurez-vous que cette valeur est définie sur **column_level_encryption**.

4. Sélectionnez **Soumettre**.

Que faire ensuite

Configurez l'objectif, l'algorithme, la longueur de la clé, le mode et l'origine de votre clé de chiffrement dans Spécifications cryptographiques pour Chiffrement de champ.

Spécifications cryptographiques pour Chiffrement de champ

Utilisez des spécifications cryptographiques pour définir l'objectif, l'algorithme, la longueur de la clé, le mode et l'origine de votre clé de chiffrement.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire de chiffrement KMF

Pourquoi et quand exécuter cette tâche

Cette procédure montre comment configurer les clés générées. Une clé de chiffrement des données (appelée clé de module) est automatiquement renseignée une fois que vous avez configuré les spécifications de chiffrement.

Pour la configuration des clés fournies par le client, reportez-vous à la section Configurer les clés fournies par le client pour Chiffrement de champ Enterprise.

Procédure

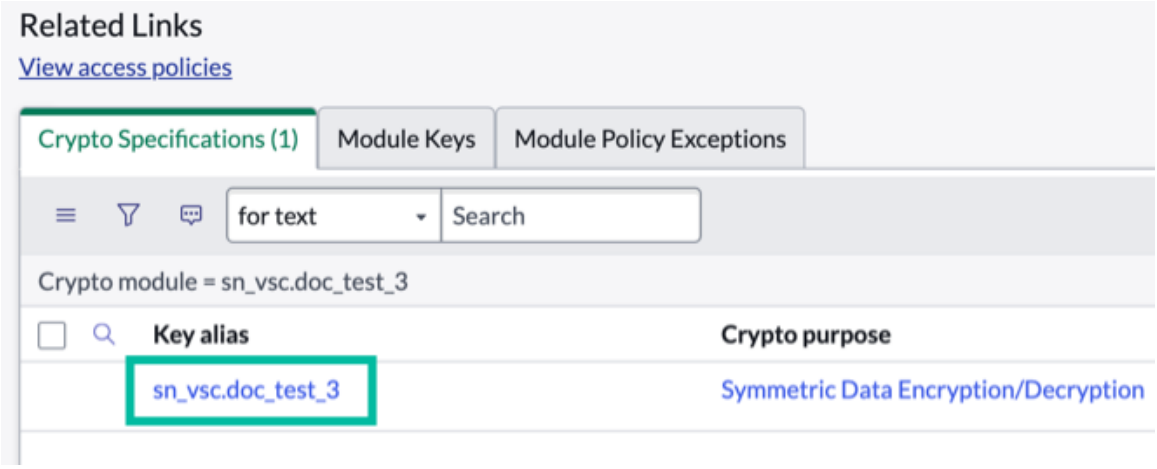
1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Modules de chiffrement de champ**.
2. Dans la liste **Modules de chiffrement** , ouvrez l'enregistrement de module que vous souhaitez configurer.

   Remarque :
   Les noms affichés dans la liste sont ajoutés avec le champ d'application, par exemple, `global.[ nom de votre module de chiffrement de champ]`.

3. Dans la liste connexe **Spécifications de chiffrement** , ouvrez l'enregistrement de chiffrement spécifique en sélectionnant le nom sous **Alias de clé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le formulaire Spécifications cryptographiques, renseignez les champs selon vos besoins.

Remarque :
Les champs sont divisés en sections. Sélectionnez les boutons **Suivant** ou **Retour** pour naviguer entre les sections.

Section	Champ	Description
Définition de l'algorithme	Module de chiffrement	Affiche le nom du module de chiffrement sélectionné.
	Objectif de chiffrement	But de l'algorithme, de la clé, de la longueur et du mode sélectionnés. Pour Chiffrement de champ, ce champ est en lecture seule et a la valeur **Chiffrement/Déchiffrement symétrique des données**.
	Algorithme	Sélectionnez un type d'algorithme utilisé pour atteindre l'objectif cryptographique. Les options disponibles sont filtrées pour s'aligner sur l'objectif cryptographique sélectionné.
Définition du cycle de vie	Concerne	Affiche la clé sélectionnée à laquelle le cycle de vie s'applique.
	Pour le champ	Sélectionnez le type de contrôle de la clé que vous souhaitez appliquer pour le cycle de vie. ○ Date d'expiration ○ Prochaine date d'activation ○ Prochaine date de destruction ○ Prochaine date de renouvellement ○ Prochaine date de rotation
	Type de clé	
	Valeur par défaut du cycle de vie	
	Ordre	Ordre dans lequel traiter l'état du cycle de vie de la clé pour la spécification de chiffrement. Les valeurs inférieures s'exécutent avant les valeurs plus élevées.
	Durée relative	Nombre d'années, de mois ou de jours pendant lesquels la clé est valide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section	Champ	Description
	Type de durée relative	Type de durée du cycle de vie. Sélectionnez parmi **Années**, **Mois** ou **Jours**.
	Opération relative	Choisissez **Avant** ou **Après**.
	Relatif à	Sélectionnez un champ auquel la durée est relative. ○ Date d'activation ○ Date compromise ○ Date de désactivation ○ Date de destruction ○ Date d'expiration ○ Date de création ○ Dernière date de renouvellement ○ Date de la dernière rotation ○ Date de révocation **Remarque :** Ce champ fonctionne avec la valeur sélectionnée dans le champ **Opération relative** .
	Type	Indiquez si la valeur du cycle de vie de la clé est relative ou absolue. **Relatif** Entrez une valeur qui dépend d'autres entrées de données dans le système, telles que la génération, l'activation et la désactivation de clés. **Absolu** Saisissez une valeur exacte, telle qu'une date.
Origine de la clé	Module de chiffrement	Affiche le nom du module de chiffrement sélectionné.
	Origine	Indique si la clé provient du client ou est fournie par le client. ○ Pour commencer, sélectionnez **ServiceNow** ○ Pour Entreprise, sélectionnez **ServiceNow** ou **Fourni par le client**
	Alias de la clé	Nom du module de chiffrement avec le champ d'application ajouté au début du nom.
	Objectif de chiffrement	Affiche le but de l'algorithme, la clé, la longueur et le mode sélectionnés. Pour Chiffrement de champ, ce champ est en lecture seule et a la valeur **Chiffrement/Déchiffrement symétrique des données**.
	Algorithme	Affiche l'algorithme utilisé pour atteindre l'objectif de chiffrement.
Création de la clé	Module de chiffrement	Affiche le nom du module de chiffrement sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section	Champ	Description
	Alias de la clé	Affiche le nom du module de chiffrement avec le champ d'application ajouté au début du nom.
	Générer la clé	Sélectionnez ce lien pour générer votre clé de chiffrement des données si vous utilisez une clé générée et non une clé fournie par le client.
	Générer automatiquement la clé	Si vous ne sélectionnez pas le lien **Générer une clé** , une clé de chiffrement des données est générée automatiquement lors de la première fois que les données doivent être chiffrées à l'aide du module de chiffrement.
	Objectif de chiffrement	Affiche le but de l'algorithme, la clé, la longueur et le mode sélectionnés. Pour Chiffrement de champ, ce champ est en lecture seule et a la valeur **Chiffrement/Déchiffrement symétrique des données**.
	Origine	Affiche la valeur sélectionnée dans la section Origine de la **clé** .
	Algorithme	Affiche l'algorithme utilisé pour atteindre l'objectif de chiffrement.

5. Sélectionnez **Accéder au module de chiffrement** pour revenir à votre enregistrement de module. Dans l'enregistrement Module, il y a maintenant une entrée dans la liste connexe **Clés de module** . Le champ **Alias de clé** de la liste connexe **Spécifications de chiffrement** est maintenant vide, car l'alias de clé a été déplacé vers la nouvelle clé de module.

Que faire ensuite

Pour plus d'informations sur l'utilisation d'une clé fournie par le client, reportez-vous à la section Configurer les clés fournies par le client pour Chiffrement de champ Enterprise.

Clés de module pour Chiffrement de champ

L'onglet Clés de module vous montre des informations de niveau résumé sur votre ou vos clés de chiffrement des données de chiffrement de champ. Vous pouvez afficher l'alias de clé, le type de clé, l'algorithme, l'état du cycle de vie de la clé et la version de la clé.

Accès aux informations clés du module

Accédez à vos clés de module à partir des enregistrements de la table Module de chiffrement [sys_kmf_crypto_module]. À partir d'un enregistrement de module de chiffrement, vous pouvez sélectionner le champ **Alias de clé** dans les enregistrements de la liste connexe **Clés de module** .

Les informations disponibles dépendent de la version active que Chiffrement de champ vous avez sur votre instance.

Chiffrement de champ Démarreur

À l'aide Chiffrement de champ de Starter, vous pouvez afficher les données d'audit de l'utilisation des clés.

Chiffrement de champ Enterprise

Vous devez effectuer des opérations de clés manuelles telles que Renouveler, Révoquer, Faire pivoter ou Suspendre, en plus d'afficher les données d'audit de l'utilisation clé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations clés du module

Les informations sur vos clés de module sont affichées dans l'enregistrement de clé de module dans les champs répertoriés ici. Ces champs sont en lecture seule et utilisés à des fins d'information uniquement.

Champ	Description
Date de création	Quand la clé de module a été générée
Date d'activation	Lorsque la clé Module a été activée.
Dernière date de renouvellement	Dernière fois que la clé de module a été renouvelée.
Date de la dernière rotation	La dernière rotation de la clé de module.
Date de désactivation	Lorsque la clé de module a été désactivée.
Date de destruction	Lorsque la clé de module a été détruite.
Prochaine date d'activation	Lorsque la clé de module sera activée.
Prochaine date de renouvellement	Lorsque la clé de module sera renouvelée.
Prochaine date de rotation	Lorsque la clé de module sera tournée.
Prochaine date de destruction	Lorsque la clé de module sera détruite.
État du cycle de vie de la clé	État actuel de la clé de module.

Exceptions de politique de cycle de vie des modules pour Chiffrement de champ

Utilisez les exceptions de politique de cycle de vie de module pour personnaliser le cycle de vie de vos clés de module.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire de chiffrement KMF

Pourquoi et quand exécuter cette tâche

Les exceptions de politique de cycle de vie des modules modifient la politique de cycle de vie des modules par rapport à la politique de cycle de vie standard au niveau de l'instance Chiffrement de champ . Par exemple, si vous avez configuré des clés symétriques limitées à un an au niveau de l'instance, vous pouvez créer une exception de politique de cycle de vie de module pour un module spécifique Chiffrement de champ afin de permettre à sa clé de rester active pendant deux ans.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Modules de chiffrement de champ**.
2. Sélectionnez l'enregistrement du module de chiffrement de champ qui nécessite une exception de politique de cycle de vie du module.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans l'enregistrement du module de chiffrement de champ, sélectionnez **Nouveau** dans la liste connexe **Exceptions de politique du module** .
4. Dans le formulaire Politique du cycle de vie de la clé, renseignez les champs selon vos besoins.

Champ	Description
Module de chiffrement	Affiche le nom du module de chiffrement de champ qui utilisera cette exception de politique.
Concerne	La clé spécifiée est renseignée automatiquement.
Type de clé	Sélectionnez le type de clé. Les politiques d'exception sont liées à une clé spécifique. Plusieurs politiques d'exception peuvent être créées par Chiffrement de champ module.
Condition de politique	Créez des conditions d'éligibilité à partir du menu déroulant et remplissez les critères de contrainte supplémentaires.
Résultat	Sélectionnez **Rejeter** pour rejeter l'utilisation de la clé ou **Suivre** pour permettre son utilisation lorsque les critères sont remplis.

5. Sélectionnez **Soumettre**.

Configurer les clés fournies par le client pour Chiffrement de champ Enterprise

Apportez votre propre clé de chiffrement des données à la plateforme au lieu d'utiliser celle qui ServiceNow génère.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire de chiffrement KMF

Pourquoi et quand exécuter cette tâche

Si vous utilisez Chiffrement de champ Enterprise, vous pouvez utiliser votre propre clé de chiffrement des données vers la plateforme plutôt qu'une clé générée par ServiceNow.

Vous devez disposer d'une clé symétrique générée en dehors de ServiceNow. Les exemples de ce document reposent sur OpenSSL. Pour plus d'informations sur OpenSSL, consultez les détails sur https://www.openssl.org . Si vous utilisez d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

Procédure

1. Dans une ligne de commande sur votre machine (exemple : Terminal), exécutez la commande suivante : `openssl rand -hex 32 -out mykey.bin`.
   Enregistrez le fichier `mykey.bin` , qui sera utilisé dans les étapes suivantes.
2. Sur votre instance, accédez à **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Paramètres de Chiffrement de champ**.
3. Remplacez le champ **Source** de clé **des clés générées par ServiceNow** par **Clés fournies par le client**.
4. Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Utilisez la clé symétrique que vous avez créée sur votre instance en procédant comme suit :

1. Configurer les propriétés de la clé fournie par le client
2. Enveloppez votre clé fournie par le client
3. Télécharger la clé fournie par le client

Configurer les propriétés de la clé fournie par le client

Examinez les propriétés système de la clé d'emballage publique éphémère que votre instance utilise pour désencapsuler les clés fournies par le client.

Avant de commencer

Rôle requis : administrateur KMF ou opérateur de chiffrement KMF

Pourquoi et quand exécuter cette tâche

Vous devez encapsuler votre clé de chiffrement de données symétriques avec une ServiceNow clé d'encapsulation publique éphémère avant de pouvoir la charger sur votre instance.

Lorsque votre clé est téléchargée dans votre instance, celle-ci la désencapsule à l'aide du côté privé de la clé publique.

Vous pouvez utiliser les propriétés système de votre instance pour définir le remplissage de clé, la taille de la paire de clés éphémères et une période de validité de clé pour cette clé publique éphémère.

Propriété système	Description	Valeur par défaut
glide.kmf.ephemeral.key_padding	Schéma de remplissage de clé pour la clé éphémère.	OAEPWithSHA256AndMGF1Rembourrage OAEP SHA256, mais SHA1 est pris en charge.
glide.kmf.ephemeral.key_size	Taille de la paire de clés éphémères.	4096 4096 bits, mais 2048 bits sont également pris en charge.
Glide.kmf.ephemeral.key_period	Période pendant laquelle la paire de clés éphémères est valide.	02:00:00 2 heures

Procédure

Contactez ServiceNow le support technique si vous devez modifier l'une de ces propriétés.

Remarque :
Ces propriétés système ne sont pas visibles par les administrateurs et n'apparaissent pas dans la liste des propriétés système [sys_properties]. Utilisez la table ci-dessus pour voir leurs valeurs par défaut.

Que faire ensuite

Une fois vos propriétés configurées en fonction de vos besoins, passez à Enveloppez votre clé fournie par le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enveloppez votre clé fournie par le client

Encapsulez votre clé de chiffrement de données symétriques avec une clé d'encapsulation publique éphémère avant de pouvoir la charger sur votre instance.

Avant de commencer
Rôle requis : administrateur KMF ou opérateur de chiffrement KMF

Vous devez disposer d'une clé de chiffrement de données symétrique dans un `.bin` pour exécuter ces étapes. Pour obtenir des instructions sur ce processus, reportez-vous à la section Configurer les clés fournies par le client pour Chiffrement de champ Enterprise.

Important :
Votre clé de chiffrement symétrique des données doit être au format binaire (. BIN). Si un autre format est utilisé, le message d'erreur suivant s'affiche :

Échec de la validation du jeton. Veuillez attacher à nouveau le jeton non modifié.

Pourquoi et quand exécuter cette tâche
Pour modifier les propriétés facultatives qui contrôlent la taille, l'algorithme de remplissage et la période de validité de la clé, reportez-vous à la section Configurer les propriétés de la clé fournie par le client.

Vous devez disposer d'un outil cryptographique pour encapsuler votre clé. L'exemple de ce document utilise OpenSSL 1.1. Pour plus d'informations sur OpenSSL, consultez les détails sur https://www.openssl.org . Si vous utilisez d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Modules de chiffrement de champ**.
2. Ouvrez un module de chiffrement de champ que vous avez précédemment créé.

   Remarque :
   Si vous n'avez pas encore créé de module de chiffrement de champ, vous pouvez en créer un en suivant les étapes de la section Configurer les Chiffrement de champ modules.

3. Dans la liste connexe **Module** , ouvrez l'enregistrement cryptographique spécifique en sélectionnant le nom sous **Alias de clé**.
4. Sélectionnez le bouton **suivant** jusqu'à ce que vous atteigniez la section **Origine de la clé** .
5. Vérifiez que la valeur du champ **Origine** est **Télécharger la clé fournie par le client**.
   Si ce n'est pas le cas et que vous ne pouvez pas choisir cette valeur, reportez-vous aux étapes 3 à 5 de la section Configurer les clés fournies par le client pour Chiffrement de champ Enterprise.
6. Dans le champ **Alias de clé** , créez un alias.
   Votre clé utilise cet alias une fois qu'elle est chargée.
7. Sélectionnez **Suivant**.
8. Sélectionnez le lien dans le champ Télécharger la **clé d'encapsulation** .

   Un fichier `token_publickey` est téléchargé sur votre ordinateur. Ne renommez pas ce fichier.

9. Sur votre ordinateur local, décompressez et ouvrez le dossier `token_publickey` .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez voir un fichier de jeton d'importation (.txt) et un fichier de clé publique (. PEM) dans ce dossier.

10. Déplacez votre clé de chiffrement des données symétriques que vous avez générée dans ce dossier.
11. Copiez le nom du fichier token_publickey dans votre presse-papiers.
12. Ouvrez une session de terminal et accédez au dossier token_publickey .
13. Entrez la commande suivante :

> **Important :**
> Remplacez tout texte entre crochets (<>) par vos noms et informations de fichier spécifiques. Utilisez la table d'exemples de commandes d'encapsulation de touches suivante comme guide.

```
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>. PEM -in <keyname.bin> -out wrapped_key_material -pkeyopt rsa_padding_mode : oaep -pkeyopt rsa_oaep_md :sha<128 ou 256>
```

Exemples de commandes d'encapsulation de clé

Directions	Commande	Exemple
Saisissez le publickey_<keyname>. PEM	openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>. PEM	openssl pkeyutl -encrypt -pubin -inkey publickey_567898643ffff. PEM
Entrer le nom de votre clé de chiffrement de données symétriques	-in <keyname.bin>	-in mykey.bin
Entrez la commande <-out> spécifiez si le matériel de clé encapsulé doit être 128 bits ou 256 bits	-out wrapped_key_material -pkeyopt rsa_padding_mode :oaep -pkeyopt rsa_oaep_md :sha256	N/A

Que faire ensuite

Maintenant que votre clé est encapsulée, vous pouvez la télécharger sur votre instance en suivant la procédure de la section Télécharger la clé fournie par le client.

Télécharger la clé fournie par le client

Chargez votre clé de chiffrement des données symétriques encapsulées dans votre instance pour commencer à l'utiliser chiffrement de travail.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire de chiffrement KMF

Pourquoi et quand exécuter cette tâche

> **Remarque :**
> Si vous ne souhaitez pas fournir votre propre clé, vous pouvez suivre les étapes de la section Configurer les Chiffrement de champ modules .ServiceNow Vous ne pouvez pas révoquer une clé fournie par le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Modules de chiffrement de champ**.
2. Ouvrez un module de chiffrement de champ dans lequel vous souhaitez utiliser votre clé.
3. Dans la liste connexe **Module** , ouvrez l'enregistrement cryptographique spécifique en sélectionnant le nom sous **Alias de clé**.
4. Sélectionnez le bouton **suivant** jusqu'à ce que vous atteigniez la section **Origine de la clé** .
5. Vérifiez que la valeur du champ **Origine** est **Télécharger la clé fournie par le client**.
   Si ce n'est pas le cas et que vous ne pouvez pas choisir cette valeur, reportez-vous aux étapes 3 à 5 de la section Configurer les clés fournies par le client pour Chiffrement de champ Enterprise.
6. Confirmez que vous avez une valeur dans le champ **Alias de clé** .
7. Sélectionnez **Suivant**.
8. Sélectionnez le lien **Télécharger la clé fournie par le client** .
   Ce lien doit apparaître sous le lien **Télécharger la clé encapsulée** que vous avez sélectionné lors de l'encapsulation de votre clé.
9. Sélectionnez **Parcourir**, puis sélectionnez deux fichiers :
   a. Fichier wrapped_key_material
   b. Fichier « jeton d'importation »
10. Sélectionnez **OK**.

Résultats

Un message de confirmation indique un chargement réussi de la clé fournie par le client. La clé est également répertoriée dans la liste connexe **Clés de module** avec une **origine** de la clé fournie par le client.

Maintenant que votre clé de chiffrement est configurée, vous pouvez commencer à spécifier quels champs et pièces jointes sont chiffrés. Pour plus de détails, voir Configurer des configurations de champs chiffrés pour les champs ou les pièces jointes.

Configurer des configurations de champs chiffrés pour les champs ou les pièces jointes

Créez une configuration de champs chiffrés pour spécifier quels champs sont chiffrés dans une table et si les pièces jointes de ces tables sont chiffrées.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire cryptographique KMF, administrateur de sécurité

Vous devez disposer d'un module de chiffrement de champ configuré avec une ServiceNow clé fournie par le client. Si vous n'avez pas encore configuré de module, reportez-vous à la section Configurer les Chiffrement de champ modules.

Procédure

1. Assurez-vous d'être dans le même périmètre de l'application que la table que vous souhaitez chiffrer.
2. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.
3. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans le formulaire **Configuration des champs chiffrés** , renseignez les champs selon vos besoins.

Champ	Valeur
Type	Sélectionner **colonne** ou **pièce jointe** **Remarque :** Le chiffrement des pièces jointes n'est disponible qu'avec Chiffrement de champ Enterprise.
Table	Sélectionnez la table dont les champs ou les pièces jointes seront chiffrés.
Colonne	Si vous avez choisi **Colonne** dans le champ **Type** , sélectionnez les champs à chiffrer. **Remarque :** Si le champ que vous souhaitez chiffrer n'est pas disponible, ce type n'est peut-être pas pris en charge. Les types de champs pris en charge sont les suivants : ○ Chaîne (y compris UTF-8 complet) ○ Date ○ Date/Heure ○ URL ○ HTML ○ Journal ○ Traduit ○ E-mail ○ Téléphone
Actif	Indique si la configuration est active. **Important :** Lorsqu'elle est active, votre instance chiffre activement les nouvelles données dans les champs ou pièces jointes sélectionnés. Les utilisateurs n'auront pas accès à ces données à moins d'en avoir l'autorisation via une politique d'accès au module associée. Ne vérifiez pas si le champ n'est pas encore prêt à commencer le chiffrement et l'application des politiques d'accès au module. Pour vous assurer que les données historiques sont chiffrées après qu'une configuration de champs chiffrés est active, vous devez exécuter une tâche de chiffrement en masse sur la colonne. Pour plus d'informations, consultez « Planifier le chiffrement, le déchiffrement ou la nouvelle saisie en masse ».
Module de chiffrement	Module de chiffrement de champ utilisé par cette configuration de champ chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Fonction de message REST	Sélectionnez **Module unique** pour vous assurer que tous les champs ou pièces jointes sont chiffrés par un seul module de chiffrement de champ. Sélectionnez **Module multiple** pour permettre l'utilisation de différents modules de chiffrement de champ pour différentes lignes d'une colonne ou différentes pièces jointes. Pour plus d'informations sur la configuration multi-modules, reportez-vous à la section .
Préservation de l'égalité d'algorithme	Affiche si la **préservation de l'égalité** est activée dans le module de chiffrement de champ sélectionné dans le champ **Module de chiffrement** .

5. Sélectionnez **Soumettre**.

Configurer des configurations de champs chiffrés multimodules

Créez une configuration de champs chiffrés qui utilise plusieurs modules de chiffrement.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire cryptographique KMF, administrateur de sécurité

Vous devez disposer d'un module de chiffrement de champ configuré avec une ServiceNow clé fournie par le client. Si vous n'avez pas encore configuré de module, reportez-vous à la section Configurer les Chiffrement de champ modules.

Pourquoi et quand exécuter cette tâche

Utilisez plusieurs modules de chiffrement pour une configuration de champ chiffré unique afin de chiffrer différentes lignes dans une colonne (ou différentes pièces jointes dans la même table) à l'aide de différentes clés de module. Par exemple, des utilisateurs ayant des rôles différents peuvent chiffrer des données sur la même table, tout en étant empêchés de déchiffrer les données chiffrées des autres.

⚠ Avertissement :

Notez ces limitations sur la configuration des champs chiffrés multi-modules avant de poursuivre :

- Le chiffrement en masse n'est pas pris en charge pour les configurations de champs chiffrés à plusieurs modules.
- Vous ne pouvez pas changer la configuration d'un champ de plusieurs modules à un module unique. Au lieu de cela, vous devez désactiver la configuration de champ multi-module et en créer une nouvelle à module unique.
- La clé de module utilisée par une configuration de champ multi-modules est déterminée par le premier utilisateur à entrer les données dans un champ. Étant donné que le module de chiffrement de champ est défini pour chaque enregistrement, les champs d'une liste peuvent être chiffrés par différents modules de chiffrement de champ. Toutefois, au sein d'un seul enregistrement, le champ ne peut être chiffré que par un seul module de chiffrement de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Vérifiez que vous êtes dans le même périmètre de l'application que la table que vous souhaitez chiffrer.
2. Confirmez que les modules de chiffrement de champ que vous souhaitez utiliser sont créés.
   Si vous ne l'avez pas fait, reportez-vous à la section Configurer les Chiffrement de champ modules.
3. Vérifiez que chacun de vos modules a une politique d'accès au module.
   Si vous ne l'avez pas fait, reportez-vous à la section Configurer les politiques d'accès aux modules pour le chiffrement de champ.
4. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.
5. Ouvrir ou créer un enregistrement de configuration de champ chiffré.
6. Dans le champ **Méthode** , sélectionnez **Modules multiples**.
7. Sélectionnez **Colonne** ou **Pièce jointe** dans le champ **Type** , en fonction de vos besoins.
8. Sélectionnez une table dans le champ **Table** et une colonne dans le champ **Colonne** , le cas échéant.
9. Sélectionnez **Soumettre**.

Résultats

Une fois l'enregistrement enregistré et le champ **Actif** activé, les nouvelles données créées pour le champ spécifié sont chiffrées avec la clé de module du module de chiffrement de champ pertinent. Lorsqu'un utilisateur ayant le rôle dans la politique d'accès au module « A » écrit dans la table spécifiée, les données sont chiffrées avec la clé de module des modules de chiffrement de champ « A ». Dans ce cas, seuls les utilisateurs ayant le même rôle sont en mesure de déchiffrer ces données.

Example: Chiffrement de la colonne Brève description de la table Incident à l'aide d'une configuration de champs chiffrés à plusieurs modules

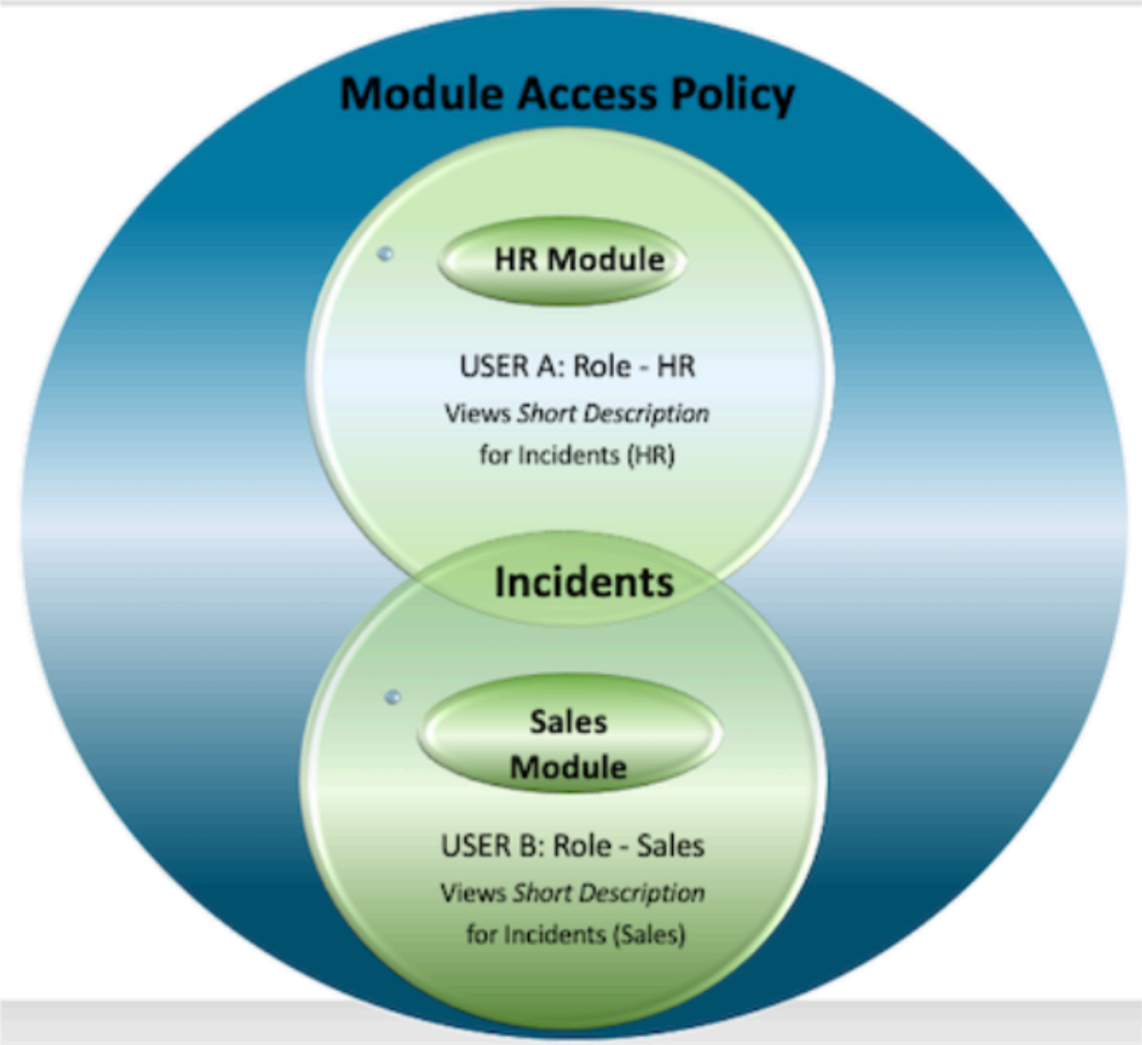
1. Créez deux modules de chiffrement de champ, désignés par A et B dans cet exemple.
2. Pour chaque module de chiffrement de champ, créez une politique d'accès au module (MAP A et B).
   a. Pour le module de chiffrement de champ A, donner aux utilisateurs ayant un rôle RH l'accès à la politique d'accès au module A.
   b. Pour le module de chiffrement de champ B, donnez aux utilisateurs ayant un rôle de vente l'accès à la politique d'accès au module B.
3. Créez un enregistrement de configuration de champ chiffré spécifiant la colonne Brève description dans la table Incident et assurez-vous de sélectionner **plusieurs modules** dans le champ **Méthode** .
4. A deux utilisateurs :
   - Une avec le rôle RH lié à la CARTE A et au module de chiffrement de champ A (utilisateur A)
   - Une avec le rôle de vente lié à la CARTE B et au module de chiffrement de champ B (utilisateur B)

   Créez un enregistrement d'incident avec une valeur de description brève. Demandez aux deux utilisateurs de consulter la liste des incidents.
   a. La description brève de l'enregistrement d'incident créé par l'utilisateur A est chiffrée avec la clé du module de chiffrement de champ A.
   b. La brève description de l'enregistrement d'incident créé par l'utilisateur B est chiffrée avec la clé du module de chiffrement de champ B.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Les utilisateurs disposant des rôles RH et Ventes ont accès aux incidents. Seul un utilisateur ayant le rôle RH peut déchiffrer et afficher la brève description des incidents créés par l'utilisateur A (qui avait le rôle RH). Seuls les utilisateurs disposant du rôle Ventes peuvent déchiffrer et afficher les brèves descriptions des incidents créés par l'utilisateur B (qui a le rôle Ventes).



Traduction automatique

Configurer les politiques d'accès aux modules pour le chiffrement de champ

Créez une politique d'accès au module pour contrôler quels utilisateurs, scripts ou processus système peuvent chiffrer ou déchiffrer les données chiffrées par un module de chiffrement de champ.

Avant de commencer

Rôle requis : administrateur KMF ou gestionnaire cryptographique KMF, administrateur de sécurité

Vous devez disposer d'un module de chiffrement de champ publié pour utiliser ce processus. Si vous ne l'avez pas fait, reportez-vous à la section Configurer les Chiffrement de champ modules.

Pourquoi et quand exécuter cette tâche

Les politiques d'accès aux modules (MAP) sont les contrôles d'accès que vous appliquez à vos modules de chiffrement de champ pour définir quels utilisateurs, scripts ou

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

processus système peuvent chiffrer ou déchiffrer des données. Configurez des MAP pour les utilisateurs (via des rôles), les scripts ou les processus s'exécutant dans le contexte « système ». Sans MAP, les utilisateurs, les scripts ou les processus système ne sont pas en mesure de chiffrer ou de déchiffrer les données, ce qui peut entraîner un dysfonctionnement des processus de workflow de bout en bout.

Les MAP sont distinctes des listes de contrôle d'accès (ACL), mais peuvent être utilisées en combinaison avec elles. Voir Explorer Chiffrement de champ pour plus d'informations sur l'objectif des MAP.

Pour Chiffrement de champ Enterprise, examinez pour déterminer quels utilisateurs, scripts ou processus système ont besoin d'une MAP.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
2. Sélectionnez **Nouveau**.
3. Dans le formulaire Politique d'accès au module, renseignez les champs selon vos besoins.

Champ	Description
Nom de la politique	Nom de votre MAP
Module de chiffrement	Sélectionnez le module de chiffrement de champ à régir par cette MAP.
Spécification de chiffrement	Facultatif. Sélectionnez ou créez une nouvelle spécification cryptographique pour cette MAP. Ce champ s'affiche uniquement lorsque le champ **Spécifier l'objectif** est activé.
Type	Décidez qui ou quoi doit avoir accès à cette MAP pour chiffrer ou déchiffrer des données. **Champ d'application** Tout élément se trouvant dans le périmètre de l'application spécifié a accès à cette MAP. **Rôle** Seuls les utilisateurs ayant le rôle spécifique peuvent accéder à cette MAP. **Script** Assurez-vous qu'un script spécifié peut accéder à cette MAP. **Accès au système** Permet aux processus s'exécutant dans un « contexte système » d'accéder à cette MAP. **Échange de ressources** Permet à la fonctionnalité d'échange de ressources d'accéder à cette MAP. Pour plus d'informations sur le fonctionnement de ces différents types de MAP, reportez-vous à la section Explorer Chiffrement de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Périmètre cible	Sélectionnez un périmètre auquel cette MAP s'applique. Ce champ s'affiche uniquement si le champ **Type** est défini sur **Périmètre**.
Spécifier l'objectif	Facultatif. Activez cette option pour afficher le champ **Spécification de chiffrement** sur le formulaire. Activez cette option pour configurer des opérations granulaires, telles que la possibilité pour certains utilisateurs de chiffrer, mais pas de déchiffrer.
Opération granulaire	Facultatif. Sélectionnez l'objectif cryptographique de la spécification cryptographique. Les valeurs disponibles dépendent du type de spécification de chiffrement sélectionné. Par exemple, vous pouvez spécifier que cette MAP permet uniquement aux utilisateurs de chiffrer, mais pas de déchiffrer, ou l'inverse, ou les deux. Ce champ s'affiche uniquement s'il y a une valeur dans le champ **Spécification de chiffrement** . ○ Si un utilisateur dispose d'un accès de chiffrement, mais pas d'un accès de déchiffrement, le champ s'affiche en mode d'édition et les données saisies s'affichent sous forme d'astérisques. ○ Si un utilisateur dispose d'un accès de déchiffrement, mais pas d'un accès de chiffrement, le champ affiche les données déchiffrées en mode lecture seule. ○ Si un utilisateur dispose d'un accès de chiffrement et de déchiffrement, les fonctionnalités de lecture et d'écriture sont disponibles pour le champ chiffré.
Rôle cible	Sélectionnez quel rôle doit avoir accès à cette MAP. Ce champ s'affiche uniquement lorsque le champ **Type** est défini sur **Rôle**
Table de scripts	Sélectionnez le type de script qui s'applique à cette MAP : ○ Contrôle d'accès ○ Concepteur d'activité ○ Règle métier ○ Action sur e-mail entrant ○ Créateur d'enregistrement ○ Exécution de script planifiée ○ Script Include ○ Action d'interface utilisateur ○ Widget ○ Activité du workflow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ce champ s'affiche uniquement si le champ **Type** est défini sur **Script**.
Script cible	Choisissez le script spécifique de la table de types sélectionnée dans le champ **Table de scripts** qui doit avoir accès à cette MAP. Ce champ s'affiche uniquement si le champ **Type** est défini sur **Script**.
Vérifier la version du script	Lorsque cette option est sélectionnée, le système vérifie la version du script qui est exécutée avec la version spécifiée dans le champ **Script cible** . Si les versions sont différentes, l'administrateur en est informé. Ce champ s'affiche uniquement si le champ **Type** est défini sur **Script**.
Type d'approbation	Sélectionnez **Ponctuel** ou **Récurrent** : **Unique** Permet de partager en toute sécurité la clé de chiffrement des données symétriques du module de chiffrement de champ associé avec l'instance cible une seule fois. **Récurrent** Permet de partager de façon récurrente et en toute sécurité la clé de chiffrement des données symétriques dans le module de chiffrement de champ associé avec l'instance cible. Ce champ s'affiche uniquement si le champ **Type** est défini sur **Échange de ressources**.
Hôte de l'instance cible	Entrez l'URL de l'instance cible à laquelle la clé de chiffrement de données symétrique du module de chiffrement de champ associé est envoyée. Ce champ s'affiche uniquement si le champ **Type** est défini sur **Échange de ressources**.
Emprunt d'identité	Lorsque cette option est activée, un utilisateur empruntant l'identité d'un autre utilisateur obtient toutes les autorisations MAP des deux utilisateurs. Si cette option est désactivée, un utilisateur empruntant l'identité d'un autre utilisateur ne dispose que des autorisations MAP qui lui ont été accordées avant l'emprunt d'identité.
Actif	Activez cette MAP.
Résultat	Sélectionnez l'une des options suivantes : **Trace** Permet l'accès et surveille l'utilisation du MAP. **Refuser** Rejette l'accès sauf si un autre MAP accorde l'accès. **StrictReject**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Refuse l’accès en toutes circonstances, même si un autre MAP accorde l’accès.

4. Sélectionnez **Soumettre**.

Migration vers Chiffrement de champ Enterprise

Travaux planifiés : migrez vos clés et vos données chiffrées de la prise en charge du chiffrement vers Chiffrement de champ Enterprise.

Vous pouvez passer en revue les travaux planifiés en accédant à **Sécurité de système** > **Paramètres de sécurité élevée** > **Tâches de Sécurité**:

- **autoKeyMigration** : migre les clés de contexte de chiffrement vers Cadre de travail de gestion des clés les clés de module de chiffrement (KMF).
- **autoDataMigration** : migre les données que vous avez déjà chiffrées pour utiliser la clé de KMF module de chiffrement.

Vous pouvez modifier le moment d’exécution de ces travaux planifiés et les mettre en pause ou les redémarrer à tout moment.

Vérifiez que les configurations de champs chiffrés utilisent vos clés de module nouvellement migrées en accédant à **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**. Recherchez les éléments suivants :

- Le champ **Méthode** est **un module unique**.
- Le champ **Module de chiffrement** est renseigné avec le nom du module de chiffrement que le système crée automatiquement. Vous pouvez examiner ce module et la politique d’accès au module, qui sont tous deux actifs et publiés.

Chiffrement de champ Enterprise et les clones système

S’il Chiffrement de champ Enterprise est installé sur votre instance, une nouvelle clé de chiffrement du module de chiffrement de champ est automatiquement générée sur l’instance de clone cible dans le cadre du processus de clonage. Ces clés sont générées pour tous les modules auxquels l’utilisateur a accès et qui n’ont pas déjà de clé.

Pour cette raison, les modules de chiffrement de champ sur l’instance de clone cible peuvent avoir deux clés de chiffrement de module présentes :

- Une clé de chiffrement de module actif. Il s’agit de la nouvelle clé générée après le clone, à condition que le module soit accessible à l’utilisateur et qu’il n’ait pas de clés antérieures.
- Une clé de module de chiffrement désactivée (issue du transfert d’échange de clés automatisé)

  La clé de chiffrement du module actif est utilisée pour chiffrer les données insérées selon les besoins sur l’instance de clone cible. Le module désactivé est utilisé pour déchiffrer les données existantes qui ont été clonées dans le cadre du clone système.

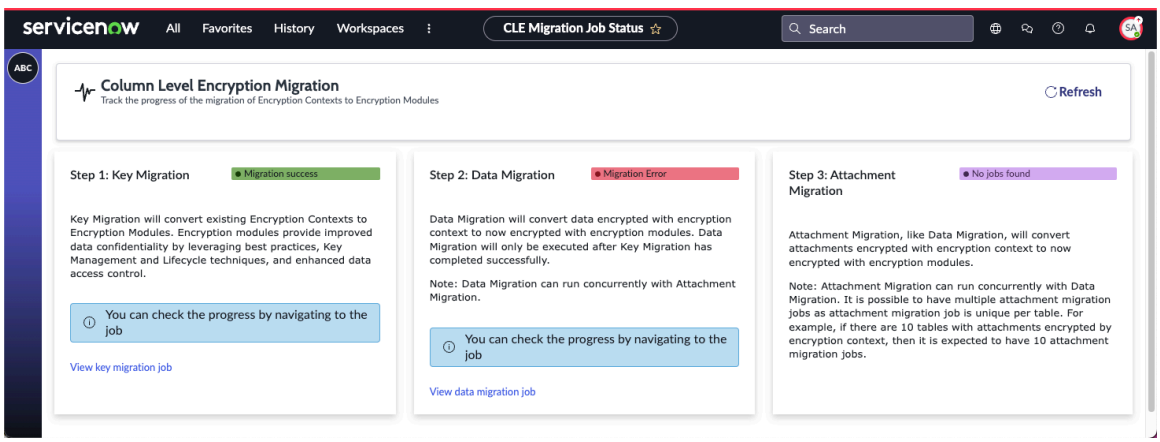
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour utiliser une seule clé pour déchiffrer et chiffrer toutes les données, vous pouvez exécuter une tâche de renouvellement de saisie de module. Pour plus d'informations sur les tâches de renouvellement de saisie de module, voir Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse.

Chiffrement de champ Page État de la migration

Utilisez la page État de la migration pour suivre la migration des contextes de chiffrement vers les modules de chiffrement.

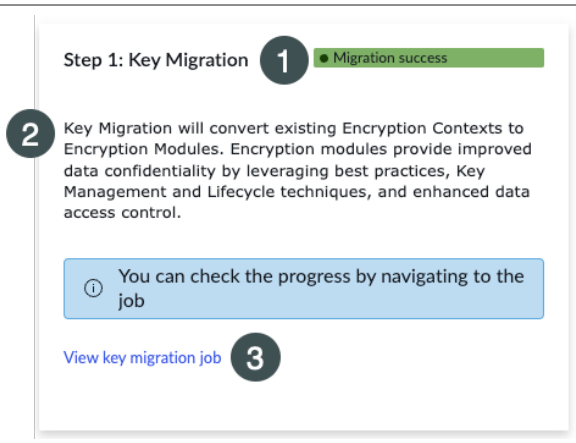


La Chiffrement de champ page Migration affiche l'état des étapes impliquées dans la migration des contextes de chiffrement vers les modules de chiffrement. Chacune des trois sections affiche l'état d'une étape spécifique du processus.

Cartes de sections de page

La page contient trois cartes représentant les étapes de la progression de la migration. Ces cartes affichent les éléments suivants :

- (1) État de l'étape en cours. Cet état indique si l'étape s'est terminée avec succès ou s'il n'y a aucune tâche à traiter.
- (2) Une description de l'étape énumérée.
- (3) Un lien vers l'enregistrement de la tâche de chiffrement [sys_mass_encryption_job] pertinente.



Migrer du chiffrement Edge vers le chiffrement de champ

Migrez du chiffrement Edge vers Chiffrement de champ pour tirer parti des dernières fonctionnalités de sécurité.

Processus de migration

Cette rubrique couvre les étapes suivantes :

1. Migrer les colonnes et la pièce jointe de Chiffrement Edge vers Chiffrement de champ.
2. Arrêtez et désactivez les serveurs proxy Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Retirer la symbolique de vos données
4. Déchiffrer les variables d'élément de Service Catalog.

Limitations

- Chiffrement de champ ne prend actuellement pas en charge la tokenisation des données de la même manière que Chiffrement Edge. Les données qui sont tokenisées via Chiffrement Edge doivent être incluses dans une configuration de champs chiffrés pour Chiffrement de champ.
- Chiffrement de champ ne prend actuellement pas en charge le chiffrement des variables d'élément de Catalogue de services.

Configurer Chiffrement de champ pour votre périphérie Champs chiffrés

Avant de migrer vos champs chiffrés Edge existants vers Chiffrement de champ, vous devez configurer le chiffrement des champs pour ces champs.

Avant de commencer

Rôle requis : admin

Ce processus suppose que vous disposez de champs chiffrés Edge existants vers lesquels Chiffrement de champ vous souhaitez migrer.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > **Modules de chiffrement** > **Tous** > **.**
2. Dans la liste Modules de chiffrement, sélectionnez **Nouveau**.
3. Renseignez ces champs dans le formulaire.

Champ	Valeur
Nom	Sélectionner un nom descriptif
Modèle de spécification de chiffrement	Modèle par défaut
État du cycle de vie du module de chiffrement	Publié
Module de chiffrement parent	column_level_encryption

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. Dans la liste connexe **Spécifications cryptographiques** , ouvrez l'enregistrement de la liste.
6. Dans l'enregistrement **Spécification de chiffrement** , sélectionnez **Suivant** trois fois pour compléter les sections de définition de l'algorithme, de définition du cycle de vie et d'origine de la clé.
   Vous n'avez pas besoin de modifier les champs de ces sections.
7. Dans le champ **Générer la clé** , sélectionnez le lien **Générer la clé** pour générer une clé.
8. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configuration des champs chiffrés**.
9. Dans la liste des configurations des champs chiffrés, sélectionnez **Nouveau**.
10. Renseignez ces champs dans le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Type	Sélectionnez Colonne ou Pièce jointe, en fonction de ce que vous souhaitez chiffrer.
Module de chiffrement	Sélectionnez le module cryptographique que vous avez créé lors des étapes précédentes.
Table	Sélectionnez la table contenant les données que vous souhaitez chiffrer.
Fonction de message REST	Sélectionner un seul module
Colonne	Sélectionnez la colonne (champ) de la table que vous souhaitez chiffrer.

Remarque :
Les données à chiffrer sont déterminées par les champs Table et Colonne. Ces champs doivent être la table et la colonne (champ) dans laquelle vous utilisez actuellement Chiffrement Edge.

11. Sélectionnez **Soumettre**.
12. Accédez à la **Tous** > **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
13. Sélectionnez **Nouveau**.
14. Renseignez ces champs dans le formulaire.

Champ	Valeur
Nom de la politique	Sélectionner un nom descriptif
Module de chiffrement	Sélectionnez le module cryptographique que vous avez créé lors des étapes précédentes.
Type	Sélectionner un rôle
Rôle cible	Sélectionnez un rôle à utiliser. Ce rôle doit être capable de chiffrer et de déchiffrer les données de la colonne.
Résultat	Sélectionnez l'action souhaitée.

15. Sélectionnez **Soumettre**.
16. Pour vérifier votre configuration, accédez à la table avec laquelle Chiffrement de champ vous souhaitez être chiffré et ouvrez un enregistrement.

    Par exemple, pour accéder à la table Utilisateur [sys_user], saisissez sys_user.list dans le filtre de navigation.

    Le champ que vous avez sélectionné pour le chiffrement dans les étapes précédentes comporte maintenant une icône de verrou en regard de l'étiquette du champ.

Résultats
Votre champ avec chiffrement Edge est prêt à être migré vers le chiffrement de champ. Pour configurer d'autres champs, répétez les étapes précédentes pour chacun de ces champs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Empêcher les utilisateurs de joindre des fichiers non chiffrés

Modifiez la propriété com.glide.encryption.enable_attachment_key_ui pour empêcher les utilisateurs ayant accès à une clé de module de chiffrement de joindre des pièces jointes non chiffrées.

Avant de commencer

Rôle requis : security_admin

Vous devez accéder au rôle security_admin en effectuant ces étapes. Pour obtenir des instructions, consultez Élever à un rôle privilégié

Par défaut, les utilisateurs qui ont accès à une clé de module de chiffrement peuvent charger des pièces jointes non chiffrées. Utilisez la `com.glide.encryption.enable_attachment_key_ui` propriété système pour modifier ce comportement.

Lors de l'attachement, vos utilisateurs voient un sélecteur d'interface utilisateur sur les enregistrements qui ont une configuration de champ chiffré à plusieurs modules. Lorsque cette propriété est définie sur faux, les utilisateurs ne voient plus d'option permettant de ne pas chiffrer une pièce jointe.

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.
2. Dans la liste des propriétés système, recherchez et ouvrez la propriété système.
3. Définissez la **valeur** de la propriété sur faux.

Utiliser Chiffrement de champ

Utilisez cette fonction Chiffrement de champ pour gérer l'accès aux données chiffrées sur vos instances.

Il existe deux méthodes de chiffrement des données de champ :

- Module unique : permet le chiffrement des données à l'aide d'un seul module de chiffrement dans une méthode déterministe.
- Multi-module : permet le chiffrement des données à l'aide de plusieurs modules de chiffrement dans une méthode non déterministe. Les conditions de ligne sont la nouvelle méthode privilégiée pour appliquer plusieurs modules à un champ. Conditions de ligne applique l'aptitude multi-module de manière déterministe.

Utilisez les liens connexes pour trouver des informations sur les tâches courantes Chiffrement de champ .

Information associée

Créer un module cryptographique pour Chiffrement de champ

Créer une spécification cryptographique pour Chiffrement de champ

Configurer des algorithmes avancés pour Chiffrement de champ Enterprise

Configurer les propriétés des clés fournies par le client

Chiffrement des champs et des pièces jointes

Chiffrement de champ Enterprise Exemples

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un module cryptographique pour Chiffrement de champ

Créez un Chiffrement de champ module cryptographique pour définir les mécanismes utilisés pour les opérations cryptographiques.

Avant de commencer

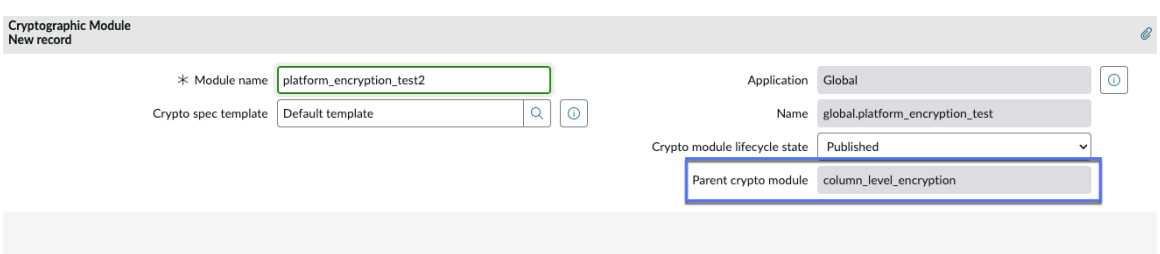
Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf_admin, security_admin, admin

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles avec Chiffrement de champ le système de base et les options de configuration supplémentaires disponibles avec Chiffrement de champ Enterprise la fonctionnalité. Chiffrement de champ Enterprise est disponible avec un abonnement payant. Consultez la rubrique Chiffrement et gestion des clés par lot pour connaître les fonctionnalités prises en charge et les options disponibles avec chaque offre. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de .

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Modules de chiffrement de champ** > **Nouveau**.



2. Remplissez les champs du formulaire.

Formulaire Module de chiffrement

Champ	Description
Nom du module	Chaîne alphanumérique à référencer lors de l'exécution de scripts.
Modèle de spécification de chiffrement	Modèle par défaut utilisé pour créer le module de chiffrement qui contient des mappages de nombreux objectifs de chiffrement sur des spécifications de chiffrement et des algorithmes recommandés.
Application	Le périmètre de l'application sélectionné.
Nom	Le nom du module de chiffrement est précédé du nom du périmètre de l'application pour éviter tout conflit avec d'autres applications incluses dans le périmètre lors de la création du module. Par exemple, si vous avez créé un module portant le nom my_crypto_module dans le périmètre de l'application global, le nom est enregistré en tant que global.my_crypto_module.
État du cycle de vie du module de chiffrement	Le terme *cycle de vie* désigne la création, l'utilisation et la désactivation d'un module cryptographique. Définir sur **Brouillon** initialement pendant la configuration. Lors de l'utilisation du module, définir sur **Publié**. Le modèle par défaut est automatiquement défini sur **Publié**.
Module de chiffrement parent	Le parent est renseigné automatiquement comme **column_level_encryption**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Envoyer**.

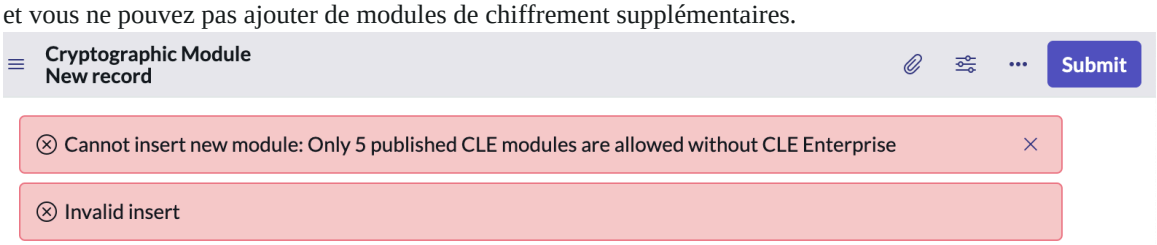
   Une fois l'envoi réussi, votre module de chiffrement est répertorié dans la table Modules de chiffrement.

> **⚠ Avertissement :**
>
> **Pour les utilisateurs de la prise en charge du chiffrement hérité :**
>
> Si vous utilisez la version non entreprise de Chiffrement de champ, vous êtes limité à cinq champs. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :
>
> Cette insertion dépasse le nombre limite de champs publiés autorisés Chiffrement de champ avec le produit d'abonnement. L'abonnement Entreprise pour Chiffrement de champ est requis pour les champs supplémentaires. Veuillez contacter l'équipe de votre compte.

Une spécification cryptographique par défaut est créée avec l'objectif de chiffrement défini sur Chiffrement/Déchiffrement de données symétriques et l'algorithme en tant que AES 256 CBC. Sélectionnez l'algorithme pour les mises à jour.

4. Pour ouvrir les options de configuration, cliquez sur le module cryptographique nouvellement créé.

> **ⓘ Remarque :**
> Un maximum de cinq Chiffrement de champ champs est autorisé avant la mise à niveau vers Chiffrement de champ Enterprise. Un message d'erreur s'affiche et vous ne pouvez pas ajouter de modules de chiffrement supplémentaires.



Que faire ensuite

Créer une spécification cryptographique pour Chiffrement de champ.

Utilisation de plusieurs modules de chiffrement

Plusieurs modules de chiffrement permettent de chiffrer les données avec plus d'un module de chiffrement. Si chaque module a sa propre politique d'accès basée sur un rôle, par exemple, des utilisateurs ayant des rôles différents peuvent chiffrer des données sur la même table, mais utiliser pour les empêcher de consulter les données chiffrées des autres.

Il existe deux façons de chiffrer des données à l'aide de plusieurs modules de chiffrement dans la plateforme :

- Conditions de ligne : permet aux administrateurs de définir le module de chiffrement à utiliser. Cette option fournit une approche déterministe et permet plusieurs configurations de champ de chiffrement (EFC) dans une seule colonne. Vous pouvez chiffrer différents enregistrements pour un champ ou une pièce jointe en configurant des clés de chiffrement distinctes pour des champs spécifiques. Pour ce faire, plusieurs configurations de champ de chiffrement (EFC) sont attribuées. Les conditions de ligne sont la méthode préférée pour chiffrer des données avec plusieurs modules. Consultez Chiffrer des données à l'aide de conditions de ligne.
- Module multiple : permet aux utilisateurs d'utiliser le module de chiffrement pour chiffrer des données. Étant donné que plusieurs modules dépendent de la sélection par l'utilisateur du module de chiffrement approprié pour chiffrer les données, cette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

configuration n'est pas déterministe et est considérée comme héritée et non préférée, même si la fonctionnalité est toujours actuellement disponible. Consultez Chiffrer les données à l'aide de la fonctionnalité Plusieurs modules.

Chiffrer des données à l'aide de conditions de ligne

Chiffrez les champs avec plusieurs modules de chiffrement de champ à l'aide de conditions de ligne pour définir les données à chiffrer et les clés de chiffrement associées. Les conditions de ligne peuvent également être utilisées pour définir les utilisateurs ayant accès à l'aide du générateur de conditions.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Remarque :

Les instructions suivantes s'appliquent lors de l'utilisation de conditions de ligne :

- Les conditions de ligne ne sont prises en charge que sur les colonnes et pièces jointes chiffrées.
- Le chiffrement en masse n'est pas disponible lors de l'utilisation de la méthode des modules de chiffrement multiples.
- Vous ne pouvez pas modifier un champ à l'aide de plusieurs modules de chiffrement pour utiliser un seul module de chiffrement.
- Les conditions de ligne permettent de chiffrer les données sur l'enregistrement principal. La remontée pas à pas n'est pas prise en charge dans le générateur de conditions.
- Conditions de ligne n'est pas pris en charge par les tables de catalogue de services suivantes :
  - Options [sc_item_option]
  - Réponse à la question [question_answer]
  - Réponse à une question de plusieurs lignes [sc_multi_row_question_answer]

Le champ est chiffré par le module de chiffrement du premier utilisateur à entrer les données. Étant donné que le module de chiffrement est défini par enregistrement, les champs d'une liste peuvent avoir différents modules de chiffrement. Au sein d'un seul enregistrement, le champ ne peut être chiffré que par un seul module.

Procédure

1. Créez plusieurs modules de chiffrement et une politique d'accès pour chacun d'eux.

   Veillez à accorder différents rôles aux différents modules de chiffrement via les stratégies d'accès.

2. Accédez à la **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.

   Si vous avez besoin de plus d'informations sur les configurations de champs chiffrés, reportez-vous à la section Définir des configurations de champs chiffrés.

3. Sélectionnez la **table** et la **colonne** de la table que vous souhaitez chiffrer.

Traduction automatique

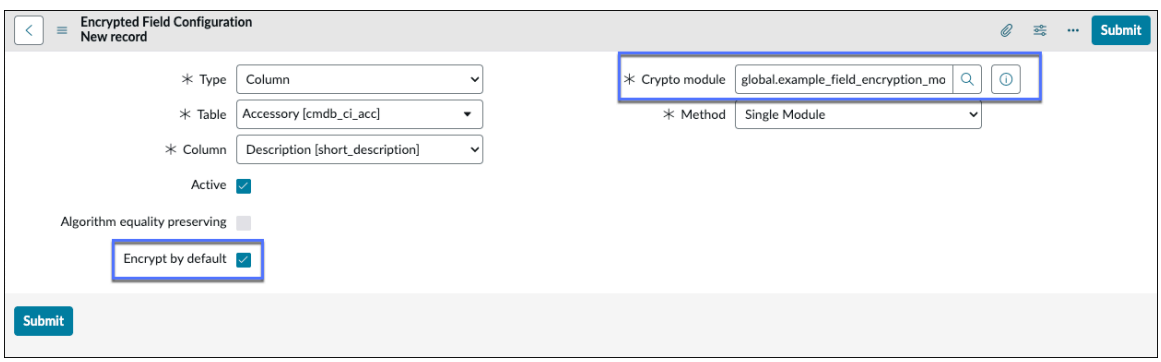
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Chiffrer par défaut** pour chiffrer les enregistrements enregistrés qui ne répondent pas à une condition de ligne définie.

   Si vous sélectionnez cette option, assurez-vous de sélectionner le **module de chiffrement** à utiliser comme module de chiffrement par défaut.

   Si cette case n'est pas sélectionnée et que les enregistrements ajoutés ne remplissent pas une condition de ligne, ils ne sont pas chiffrés.

   Par exemple, une condition de ligne peut être définie pour chiffrer les enregistrements afin de déclarer que le champ « Département » de l'enregistrement équivaut à « IT ». Ensuite, les enregistrements dans lesquels le champ « Département » n'est pas égal à « Informatique » ne sont pas chiffrés, sauf si **Chiffrer par défaut** est sélectionné.



5. Sélectionnez **Soumettre**.
6. Accéder au générateur de conditions **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** et sélectionnez la nouvelle configuration de champ chiffré (EFC).
7. Sélectionnez **Nouveau**.
8. Définissez les conditions de ligne en remplissant les champs requis.
9. Sélectionnez **Soumettre**.

Résultats

Remarque :
Répétez ce processus si nécessaire pour vous assurer que le nombre de conditions de ligne répond à vos modules de chiffrement (ECM) requis. Lorsque vous sélectionnez Chiffrer par défaut dans la configuration ECM, une condition de ligne doit également être établie pour définir l'ECM par défaut sélectionné.

Les données nouvellement créées pour le champ spécifié sont chiffrées avec la clé du module approprié. Lorsqu'un utilisateur ayant le rôle spécifié dans la politique d'accès du module A écrit dans la table spécifiée, les données sont chiffrées avec la clé du module A. Seuls les utilisateurs ayant le même rôle peuvent lire les données.

Example:

Cet exemple explique comment chiffrer le champ Description brève dans la table Incident. Cet exemple fonctionne de la même manière si vous souhaitez chiffrer un champ différent dans une table.
Pour chiffrer la brève description, procédez comme suit :

1. Créez deux modules de chiffrement de champ A et B.
2. Pour chaque module, créez une politique d'accès au module (MAP) et définissez l'accès comme suit :
   a. Module A – pour les utilisateurs ayant un rôle RH.
   b. Module B – pour les utilisateurs ayant un rôle de vente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Créez un enregistrement de configuration de champ chiffré (EFC).
   a. Accédez à la **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.
   b. Sélectionnez **Incident** dans le champ Table.
   c. Sélectionnez **Description brève** dans le champ Colonne.
   d. Cochez la case **Chiffrer par défaut** si vous devez vérifier que les enregistrements qui ne sont pas couverts par les critères du générateur de conditions sont toujours chiffrés par le module de chiffrement de champ par défaut. Ne pas sélectionner cette option signifie que les enregistrements qui ne correspondent pas aux critères du générateur de conditions ne seront pas chiffrés.

      Entrez le module de chiffrement par défaut dans le champ **Module de chiffrement** connexe.

   e. Sélectionnez **Soumettre**.
4. Créez les conditions de la ligne.
5. Exécutez la tâche de chiffrement appropriée :
   - Chiffrement en masse : exécutez cette tâche lorsqu'une nouvelle condition de ligne est créée.
   - Renouvellement de saisie en masse : exécute cette tâche lorsqu'une condition de ligne existante est modifiée.

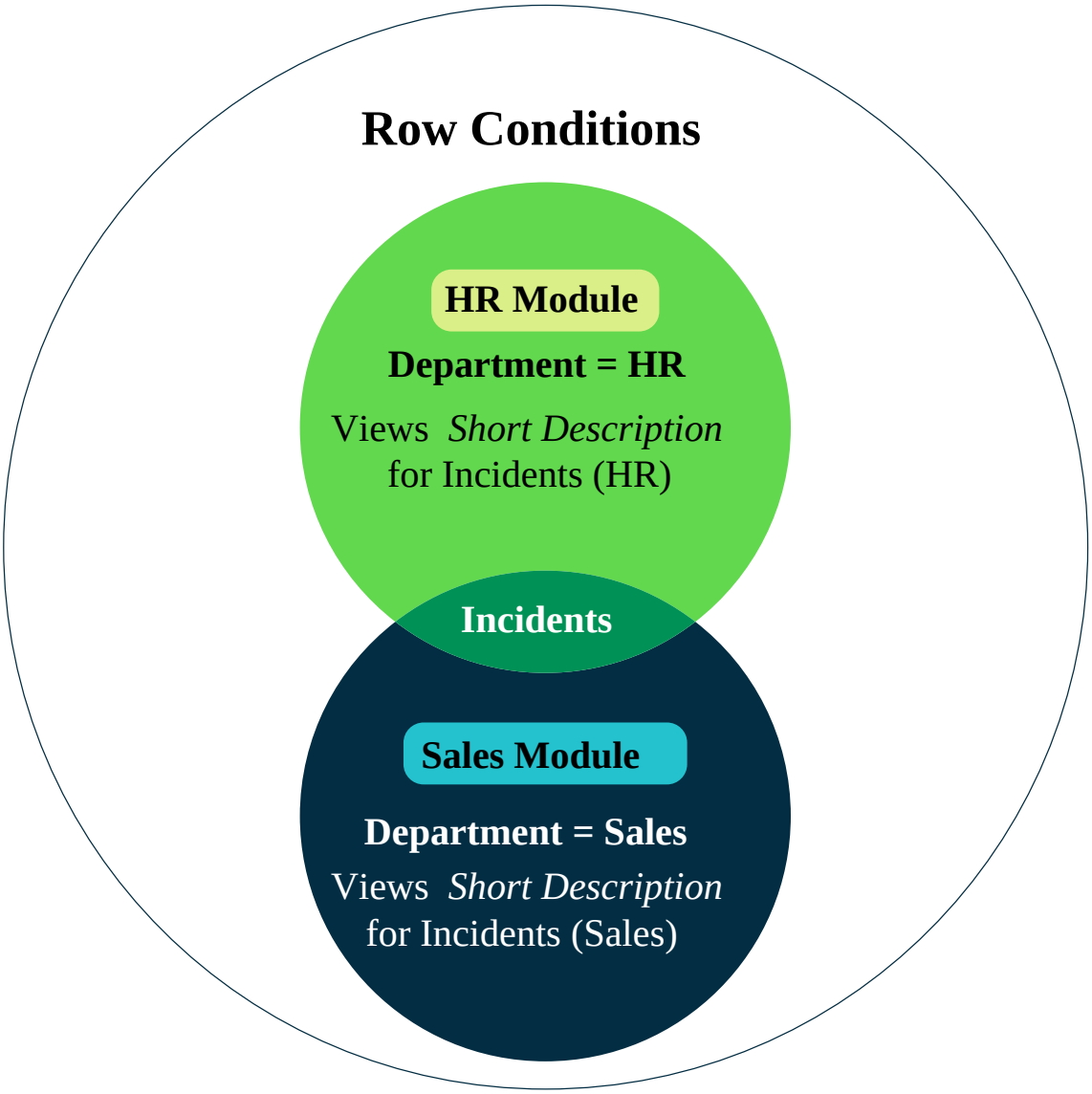
   Consultez Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse.
6. Demandez à un utilisateur du module A et à un utilisateur du module B de créer un incident avec une brève description. Demander aux deux utilisateurs d'afficher la liste des incidents.

La brève description de l'incident créée par l'utilisateur ayant le rôle RH est chiffrée par la clé du module A. La brève description de l'incident créée par l'utilisateur ayant le rôle Ventes est chiffrée par la clé du module B.

Tous les utilisateurs ayant les rôles RH et Ventes ont accès aux incidents. Toutefois, seul un utilisateur ayant le rôle RH peut déchiffrer et afficher la brève description des incidents créés par un autre utilisateur ayant le rôle RH. De même, seuls les utilisateurs disposant du rôle Ventes peuvent déchiffrer et afficher les brèves descriptions des incidents créés par l'utilisateur B, qui avait le rôle Ventes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Que faire ensuite
Effectuez l'une des opérations suivantes :

- Planifiez une tâche **de chiffrement en masse** pour mettre à jour le chiffrement du champ de condition.
- En cas de modification d'une condition de ligne existante, exécutez une tâche **de renouvellement de saisie en masse** pour chiffrer les données nécessaires avec le module de chiffrement mis à jour.

Reportez-vous à la rubrique Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse.

Chiffrer les données à l'aide de la fonctionnalité Plusieurs modules

Chiffrez les données avec plusieurs modules de chiffrement, ce qui permet à l'utilisateur de déterminer quelles clés sont utilisées pour des lignes spécifiques dans les données chiffrées.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'option Modules multiples est considérée comme non déterministe et n'est pas la méthode préférée, car l'utilisateur détermine la clé à utiliser pour un enregistrement donné. La possibilité d'utiliser plusieurs modules pour une colonne est remplacée par les conditions de ligne. Consultez Utilisation de plusieurs modules de chiffrement. Cette implémentation non déterministe est toujours prise en charge, car elle a été créée en premier et est toujours utilisée, mais il est préférable d'utiliser des conditions de ligne pour tout nouveau cas d'utilisation de plusieurs modules.

Remarque :

Seul le chiffrement sur les colonnes prend en charge plusieurs modules. Le chiffrement des pièces jointes ne le fait pas. Le chiffrement en masse n'est pas disponible lors de l'utilisation de la méthode des modules de chiffrement multiples.

Vous ne pouvez pas modifier un champ à l'aide de plusieurs modules de chiffrement pour utiliser un seul module de chiffrement.

Le champ est chiffré par le module de chiffrement du premier utilisateur à entrer les données. Étant donné que le module de chiffrement est défini par enregistrement, les champs d'une liste peuvent avoir différents modules de chiffrement. Au sein d'un seul enregistrement, le champ ne peut être chiffré que par un seul module.

Procédure

1. Créez plusieurs modules de chiffrement de champ et une politique d'accès au module (MAP) pour chacun d'eux.

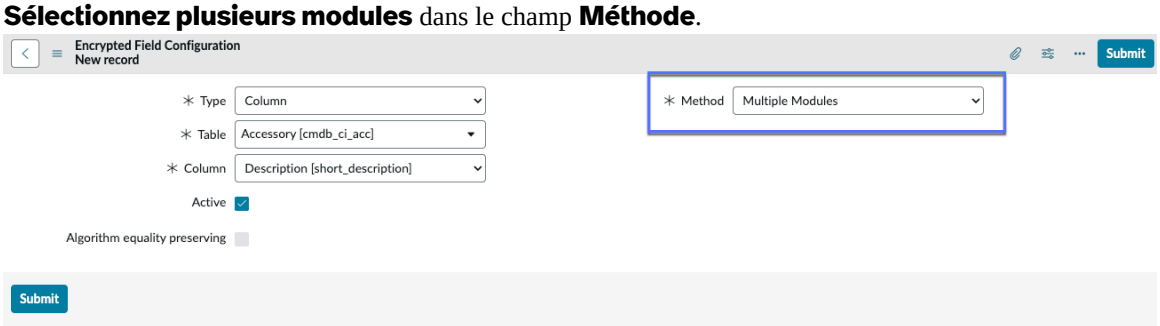
   Veillez à accorder différents rôles aux différents modules de chiffrement via les stratégies d'accès.

2. Accédez à la **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.

   Si vous avez besoin de plus d'informations sur les configurations de champs chiffrés, reportez-vous à la section Définir des configurations de champs chiffrés.

3. Dans le champ **Type** , vous devez sélectionner **Colonne**.
   Le chiffrement des pièces jointes ne prend pas en charge plusieurs modules.

4. **Sélectionnez plusieurs modules** dans le champ **Méthode**.



5. Sélectionnez la **table** et la **colonne** de la table que vous souhaitez chiffrer.

6. Sélectionnez **Soumettre**.

Résultats

Les données nouvellement créées pour le champ spécifié sont chiffrées avec la clé du module approprié. Lorsqu'un utilisateur ayant le rôle spécifié dans la politique d'accès du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

module A écrit dans la table spécifiée, les données sont chiffrées avec la clé du module A. Seuls les utilisateurs ayant le même rôle peuvent lire les données.

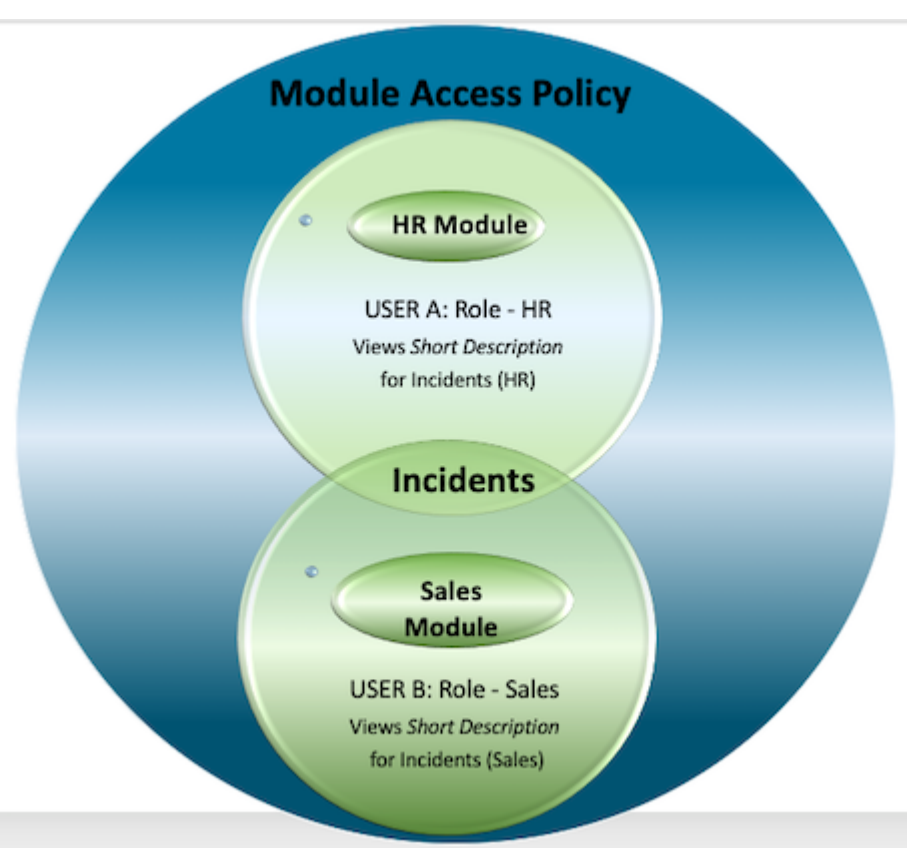
Example:
Pour chiffrer la colonne Brève description de la table Incident. Vous effectueriez les opérations suivantes :

1. Créez deux modules cryptographiques A et B.
2. Pour chaque module, créez une politique d'accès au module.

   Pour le module A, donnez accès aux utilisateurs ayant un rôle RH. Pour le module B, attribuez l'accès aux utilisateurs ayant un rôle de vente.
3. Créez un enregistrement de configuration de champ chiffré en spécifiant la colonne Brève description dans la table Incident et assurez-vous de sélectionner **plusieurs modules** dans le champ **Méthode** .
4. Demandez à deux utilisateurs, l'un avec le rôle RH (utilisateur A) et l'autre avec le rôle commercial (utilisateur B), de créer un incident avec une brève description, puis demandez aux deux utilisateurs d'examiner la liste des incidents.

   La description brève de l'incident créée par l'utilisateur ayant le rôle RH est chiffrée par la clé du module A. De même, la description brève de l'incident créée par l'utilisateur ayant le rôle Ventes est chiffrée par la clé du module B.

   Bien que tous les utilisateurs ayant les rôles RH et Ventes aient accès aux incidents, seul un utilisateur ayant le rôle RH peut déchiffrer et afficher la brève description des incidents créés par l'utilisateur A, qui avait le rôle RH. De même, seuls les utilisateurs disposant du rôle Ventes peuvent déchiffrer et afficher les brèves descriptions des incidents créés par l'utilisateur B, qui avait le rôle Ventes.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une spécification cryptographique pour Chiffrement de champ

Après avoir créé un module cryptographique, accédez à la spécification cryptographique correspondante pour définir l'algorithme.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf_admin et security_admin ou admin

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles Chiffrement de champ avec le système de base et les options de configuration supplémentaires disponibles avec Chiffrement de champ Enterprise la fonctionnalité. Chiffrement de champ Enterprise La fonctionnalité est disponible avec un abonnement payant. Consultez la rubrique Chiffrement et gestion des clés par lot pour connaître les fonctionnalités prises en charge et les options disponibles avec chaque offre. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de .

Une spécification cryptographique sera créée par le système lorsque vous créerez un module cryptographique pour Chiffrement de champ Enterprise.

Procédure

1. Accédez à la **Sécurité de système** > **Modules de chiffrement de champ** > **Tous**.
2. Sélectionnez le module cryptographique pour ouvrir les options de configuration.
   Les informations du module cryptographique sont affichées en haut de l'écran. Une spécification cryptographique de chiffrement/déchiffrement de données symétriques est créée automatiquement avec un algorithme AES 256 CBC.
3. Sélectionnez la spécification de chiffrement dans la table pour ouvrir la définition de l'algorithme.
   Pour Chiffrement de champ Enterprise voir Configurer des algorithmes avancés pour Chiffrement de champ Enterprise.
4. Cliquez sur **Suivant** pour accéder au cycle de vie de la clé.

Que faire ensuite

Effectuez l'une des opérations suivantes :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Pour plus d'informations, consultez Configurer les états clés du cycle de vie la rubrique pour compléter la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Pour obtenir des détails sur ce processus, consultez Générer une clé cryptographique ServiceNow.

Configurer des algorithmes avancés pour Chiffrement de champ Enterprise

Créez une spécification cryptographique pour définir l'algorithme d'un module cryptographique. Personnalisez les spécifications de chiffrement avec les options avancées disponibles pour Chiffrement de champ Enterprise.

Avant de commencer

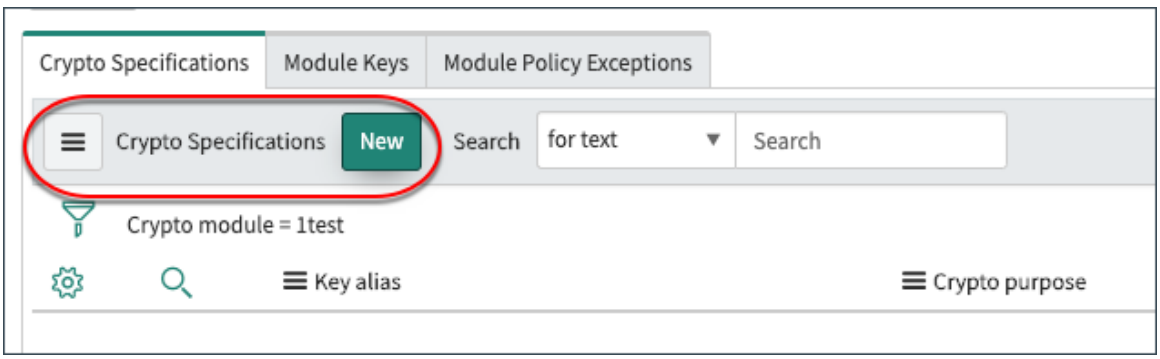
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans l'onglet **Spécifications de chiffrement (#),** cliquez sur **Nouveau**.



2. Remplissez les champs du formulaire.

Formulaire de définition de l'algorithme

Champ	Description
Module de chiffrement	Le nom du module de chiffrement sélectionné est renseigné.
Objectif de chiffrement	La valeur est **Chiffrement/Déchiffrement de données symétriques** pour Chiffrement de champ Enterprise.
Algorithme	La valeur est **AES** pour Chiffrement de champ Enterprise.
Mode d'opération	La valeur est **CBC** pour Chiffrement de champ Enterprise.
Taille	Les valeurs possibles sont **256** et **128**. **Remarque :** La taille de 256 bits est la plus sûre pour le chiffrement et est utilisée pour le chiffrement/déchiffrement de données symétriques pour Chiffrement de champ Enterprise.
Préservation de l'égalité	Option permettant d'activer le chiffrement déterministe. **Remarque :** La sélection de cette option signifie que la valeur chiffrée d'un champ doit être la même lorsque la valeur du champ reste la même. Option permettant d'activer le **chiffrement/déchiffrement de données symétriques**

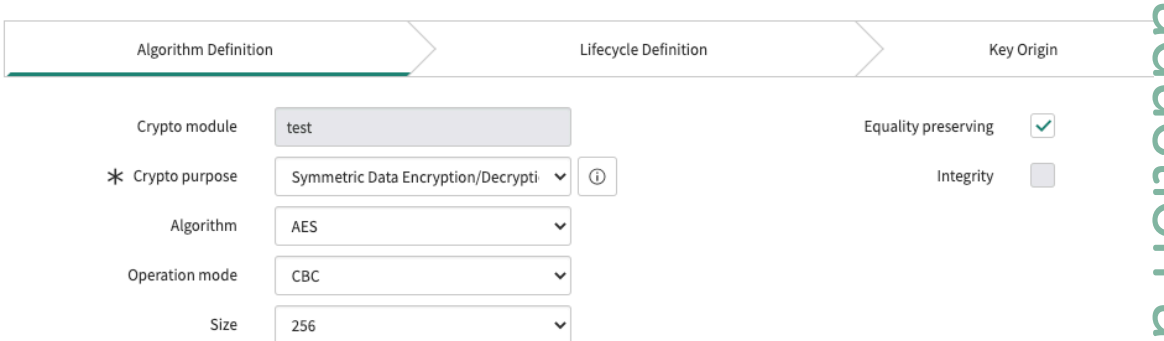
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	avec **AES** en mode **de chaînage de blocs de chiffrement (CBC).**
Intégrité	Option permettant d'assurer l'intégrité dans l'opération GCM et ne s'appliquant pas à Chiffrement de champ Enterprise la fonctionnalité.

3. Cliquez sur **Envoyer**.

L'exemple suivant montre le cryptage AES CBC-256. Lorsque Chiffrement de champ Enterprise est actif et que le module parent est column_level_encryption, seul le chiffrement/déchiffrement symétrique des données AES CBC-256 s'applique comme objectif de chiffrement. Consultez Vue d'ensemble des spécifications cryptographiques pour en savoir plus.



Que faire ensuite

Effectuez l'une des opérations suivantes :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Pour plus d'informations, consultez Configurer les états clés du cycle de vie la rubrique pour compléter la définition du cycle de vie de la clé.
- Sélectionnez **Suivant** pour créer une clé cryptographique. Consultez l'une des tâches suivantes pour la génération de clés :
  - Générer une clé cryptographique ServiceNow.
  - Configurer les propriétés des clés fournies par le client.
  - Importer la paire de clés d'encapsulation/de désencapsulation.

Utilisation des clés fournies par le client avec Chiffrement de champ Enterprise

Vous pouvez utiliser votre propre clé fournie par le client au lieu d'utiliser les clés générées par le ServiceNow® système.

Important :
Ces rubriques ne s'appliquent qu'aux instances utilisant Chiffrement de champ Enterprise, qui n'est disponible qu'avec le module `d'extension com.glide.now.platform.encryption` . Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention de ce module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avec Chiffrement de champ Enterprise vous pouvez utiliser vos propres clés pour le cryptage. Les administrateurs ont le choix d'utiliser ServiceNow® les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur le ServiceNow AI Platform.

Important :
Pour utiliser l'option de clé fournie par le client, vous devez disposer de votre propre clé cryptographique.

Une fois que vous avez votre clé, vous pouvez l'utiliser sur vos instances en suivant ces étapes.

1. **Configurer les propriétés des clés fournies par le client**

   Trois propriétés système définissent la taille, l'algorithme de remplissage et la période de validité de la paire de clés RSA d'encapsulation. Examinez ces propriétés et ajustez leurs valeurs si les valeurs par défaut ne correspondent pas à vos besoins.

2. **Enveloppez votre clé fournie par le client**

   Utilisez un outil cryptographique pour encapsuler votre clé, comme OpenSSL, pour encapsuler la clé symétrique à utiliser pour le chiffrement avec la clé publique téléchargée.

Configurer et charger la clé fournie par le client

Chargez votre clé fournie par le client et configurez le module de chiffrement pour commencer à utiliser votre clé pour le chiffrement sur votre instance.

Configurer les propriétés des clés fournies par le client

Si le module d'extension est activé, vous pouvez utiliser les Chiffrement de champ Enterprise propriétés système pour définir le remplissage des clés, la taille de la paire de clés éphémères et une période de validité des clés fournies par le client.

Chiffrement de champ Enterprise avec la gestion des clés vous permet de gérer le cycle de vie complet de vos clés de chiffrement de données. En option, vous pouvez échanger en toute sécurité des clés de chiffrement des données générées dans votre environnement.

Chiffrement de plateforme avec gestion des clés vous permet de gérer le cycle de vie complet de vos clés de chiffrement des données. En option, vous pouvez échanger en toute sécurité des clés de chiffrement des données générées dans votre environnement.

Propriétés système pour la définition d'attributs de paire de clés

Lorsque vous fournissez votre propre clé, vous devez l'envelopper avec la clé publique RSA. Trois propriétés définissent la taille, l'algorithme de remplissage et la période de validité de la paire de clés RSA d'encapsulation :

- *glide.kmf.ephemeral_key.key_padding* Contrôle le schéma de remplissage de clé pour la clé éphémère. Le schéma par défaut est OAEP SHA256, mais SHA1 est également pris en charge.
- *glide.kmf.ephemeral_key.key_size* Contrôle la taille de clé de la paire de clés éphémères. La valeur par défaut est de 4096 bits, mais les 2048 bits sont également pris en charge.
- *glide.kmf.ephemeral_key.key_validity_period* Définit la période pendant laquelle la paire de clés éphémères est valide. La valeur par défaut est de deux heures.

Une fois la clé de chiffrement des données importée dans l'instance, une clé d'encapsulation sécurisée protège les nouvelles clés de module sur l'instance. La clé d'encapsulation est une clé de chiffrement de clé d'instance (IKEK) générée par un module de sécurité matériel (HSM) sur SafeNet KeySecure. Pour plus de détails, consultez la section Clés au niveau de l'instance dans le cadre de travail de gestion des clés Types de clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Continuez vers Enveloppez votre clé fournie par le client.

Enveloppez votre clé fournie par le client

Encapsulez la clé symétrique à utiliser pour le chiffrement avec la clé publique téléchargée.

Avant de commencer

Remarque :
Cette procédure décrit les options disponibles avec KMF le système de base et les options à utiliser avec Chiffrement de champ Enterprise la fonctionnalité. Chiffrement de champ Enterprise La fonctionnalité n'est disponible que lorsque le module `d'extension com.glide.now.platform.encryption` est actif. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de .

Certaines des étapes décrites dans ce document nécessitent l'utilisation d'un outil cryptographique installé sur votre périphérique local. Les exemples de cette tâche utilisent l'outil OpenSSL. Pour en savoir plus sur cet outil, reportez-vous à la section https://www.openssl.org . Si vous utilisez d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

- Modifiez les propriétés facultatives qui contrôlent la taille, l'algorithme de remplissage et la période de validité de la clé. Consultez Configurer les propriétés des clés fournies par le client.
- Vous devez avoir votre clé symétrique (. BIN) pour le chiffrement.

Important :
Votre clé doit être au format binaire. Si un autre format est utilisé, la validation d'un jeton a échoué. Veuillez attacher à nouveau le jeton non modifié.Un message d'erreur s'affiche.

- Vous devez disposer d'un outil cryptographique pour encapsuler votre clé. Cet exemple utilise OpenSSL 1.1.

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Procédure

1. Accédez à la **Tous** > **Key Management Framework** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module de chiffrement que vous avez créé pour la clé fournie par le client dans la liste connexe Spécifications de chiffrement.
3. Vous serez dirigé vers l'étape **de création de clé** .
4. Si vous n'avez pas encore téléchargé la clé d'emballage, cliquez sur le lien pour télécharger le fichier `token_publickey<id>.zip` et enregistrez-le au même emplacement que votre clé.

   Remarque :
   Ne renommez pas le fichier `token_publickey<id>` téléchargé.

5. Décompressez le fichier sur votre réseau local.
   Le fichier zip contient deux fichiers, un jeton d'importation et une clé publique . Certificat PEM .
   Encapsulez votre clé symétrique avec la clé publique pour la chiffrer.
6. Copiez le nom du fichier `token_publickey` dans votre presse-papiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. À partir d'une ligne de commande, utilisez le nom du fichier *token_publickey* copié pour ouvrir le dossier des fichiers décompressés en tant qu'espace réservé pour la clé emballée.
8. Modifiez ce script en remplaçant les exemples par les noms de vos fichiers cryptographiques.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

Pour plus d'informations, passez en revue les commandes d'encapsulation de touches dans le tableau suivant.

Commandes d'encapsulation de touches

Directions	Commande	Exemple
Ouvrez le répertoire de fichiers dans lequel vous avez téléchargé le jeton d'encapsulation.	`cd`	token_publickey123456789 CD
Collez le nom de la clé publique. Certificat PEM .	`openssl pkeyutl -encrypt -pubin -inkey`	publickey_586798643ffff. PEM
Collez le nom de votre clé ici.	`-in`	mykey.bin
Entrez la commande <-out> et spécifiez si la clé est 128 bits ou 256 bits.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/A

9. Exécutez la commande.
   Un message système s'affiche token_publickey_<keynumber>. La clé sera générée et un fichier *wrapped_key_material* ajouté au répertoire.
10. Chargez la clé emballée.

Que faire ensuite

Revenir à Configurer et charger la clé fournie par le client pour charger votre clé emballée.

Configurer et charger la clé fournie par le client

Vous pouvez utiliser votre propre clé fournie par le client au lieu d'utiliser les clés générées par le ServiceNow® système.

Avant de commencer

Rôles requis : security_admin, sn_kmf.cryptographic_manager

Si vous ne fournissez PAS vos propres clés, vous n'avez pas besoin d'effectuer cette procédure. Pour créer un module cryptographique avec ServiceNow® des clés, accédez à Créer un module cryptographique ou Créer un module cryptographique pour Chiffrement de champ.

Remarque :
Cette procédure ne s'applique qu'aux Chiffrement de champ Enterprise fonctionnalités. Consultez Activer Chiffrement de champ pour plus d'informations.

Traduction automatique

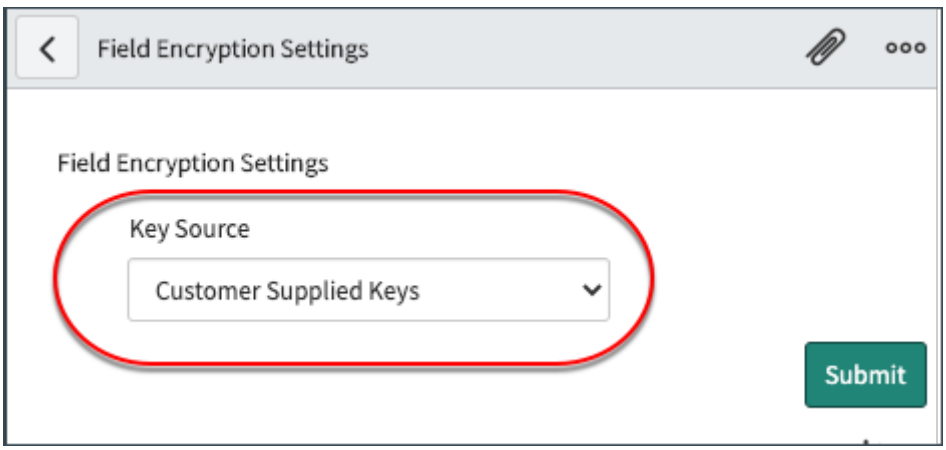
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
Vous ne pouvez pas révoquer une clé fournie par le client.

Procédure

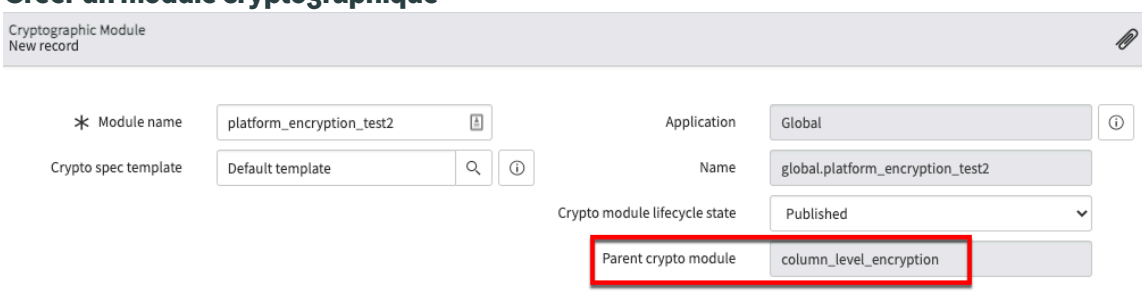
1. Accédez à la **Tous** > **Sécurité de système** > **Paramètres de Chiffrement de champ** et vérifiez que **l'option Clés fournies par le client** est sélectionnée.

Sélection de la source de clé



2. Sélectionnez **Soumettre**.
3. Retourner à **Sécurité de système** > **Modules de chiffrement de champ** > > **Créer**.

Créer un module cryptographique



4. Renseignez le formulaire du module de chiffrement comme suit :

Champs du module de chiffrement

Champ	Description
Nom du module	Entrez un nom pour le module.
Modèle de spécification de chiffrement	Le modèle de chiffrement par défaut est sélectionné.
Nom	Remplit automatiquement en fonction du nom du module et ajoute le nom au champ d'application pour s'assurer quelle application est appliquée. Dans ce cas, le périmètre global est appliqué.
État du cycle de vie du module de chiffrement	Sélectionner **Publié** pour activer le module de chiffrement.

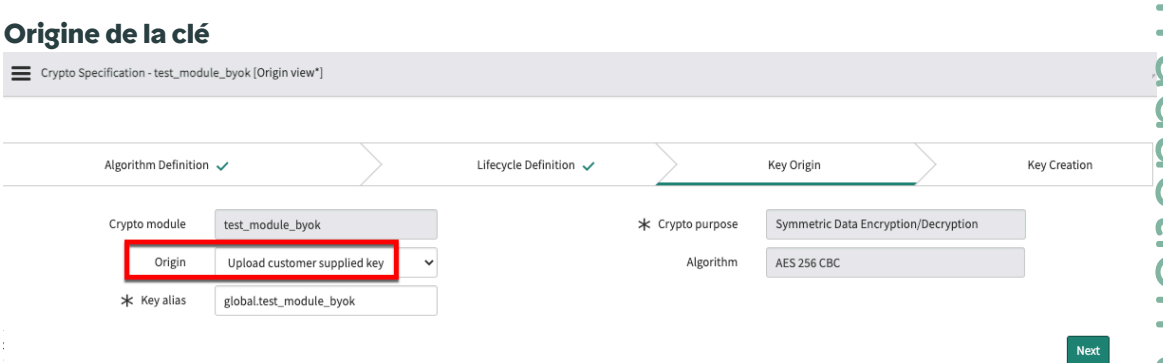
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Module de chiffrement parent	Le module parent **column_level_encryption** est sélectionné automatiquement lors de l'utilisation des clés et des modules de chiffrement fournis par le client.

5. Sélectionnez **Soumettre**.
6. Sélectionnez le module cryptographique nouvellement créé dans la table.
   Dans la liste connexe **Spécifications cryptographiques** , sélectionnez l'alias de clé généré automatiquement avec l'algorithme AES 256 CFB.

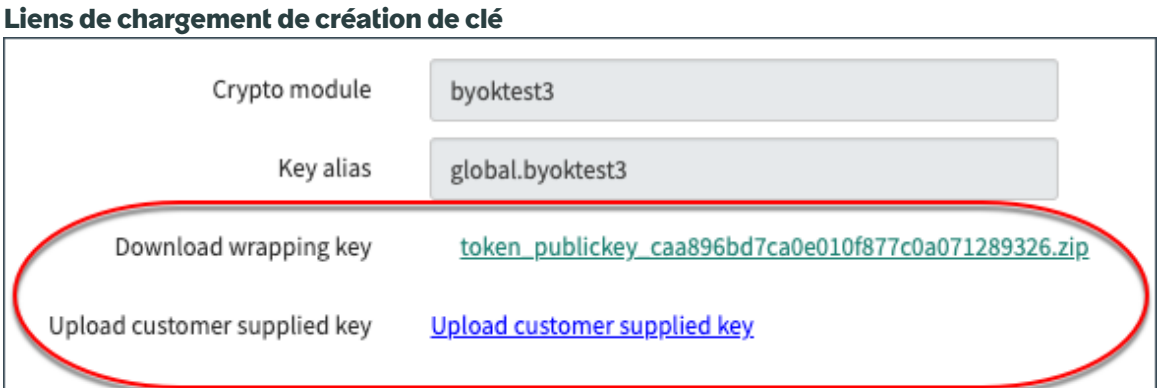
   Le système remplit automatiquement l'objectif de chiffrement et l'algorithme Chiffrement de champ et passe à l'étape **d'origine de la clé** .
7. Notez que la **clé fournie par le client** est **l'origine** et que **l'alias de clé** est déjà renseigné.



8. Sélectionnez **Suivant** pour passer à l'étape **Création de clé** .

   Il y a deux liens :

   - **Télécharger la clé encapsulée** Télécharge la clé dans un fichier zip contenant un jeton d'importation et un certificat de clé publique . PEM . Utilisez le jeton d'importation pour vérifier que l'emballage de clé a réussi, conformément aux spécifications de sécurité de l'instance. Utilisez le certificat de clé publique . Fichier PEM pour envelopper la clé fournie par votre client en toute sécurité avant de la charger avec le jeton.
   - **Télécharger la clé fournie par le client** ouvre le navigateur de fichiers pour sélectionner le jeton et la clé chiffrée que vous avez encapsulés.



9. Sélectionnez **Télécharger la clé encapsulée** pour enregistrer le jeton.

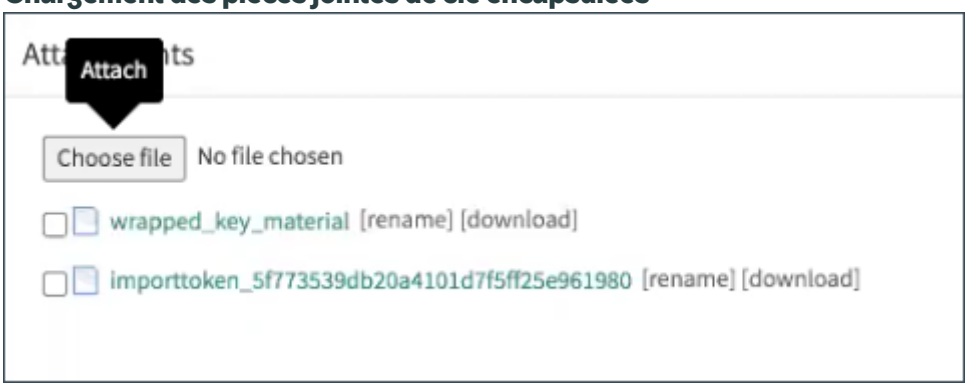
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrez le jeton au même emplacement de destination que celui où la clé est enregistrée sur votre système. Ne renommez pas le jeton téléchargé.

10. Exécutez la commande BYOK sur un terminal pour envelopper la clé.
    Pour plus d'informations, référez-vous à Enveloppez votre clé fournie par le client.
11. Sélectionnez **Télécharger la clé fournie par le client**.
12. Sélectionnez **Parcourir** pour sélectionner les deux fichiers, la clé encapsulée et le fichier de jeton.
    La fenêtre Pièces jointes affiche les deux fichiers.

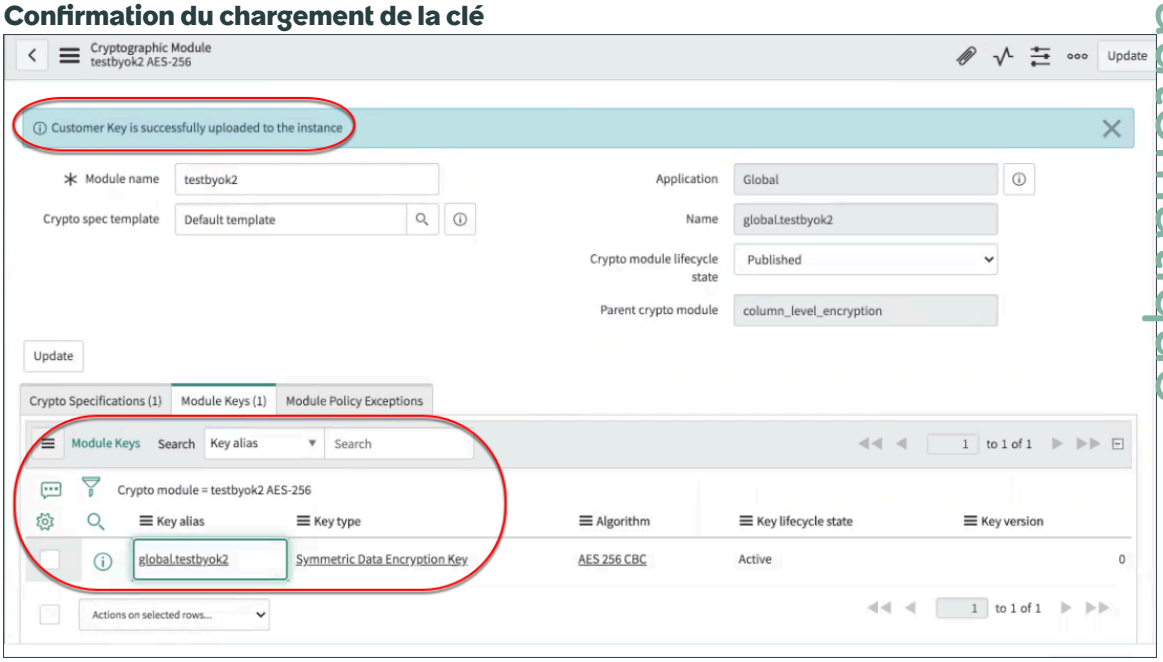
Chargement des pièces jointes de clé encapsulées



Sélectionnez un fichier à supprimer et à charger à nouveau, si nécessaire.

13. Sélectionnez **OK**.
    Vous revenez à l'écran Module de chiffrement. Un message de confirmation s'affiche pour un chargement correct de la clé client. La clé est également répertoriée dans la liste connexe Clés de module.

Confirmation du chargement de la clé



Que faire ensuite

Maintenant que vous avez terminé de configurer votre module cryptographique avec la clé fournie par le client, passez à Créer une politique d'accès au module

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrement des champs et des pièces jointes

Une fois les modules cryptographiques créés, un administrateur de sécurité peut définir la configuration des champs chiffrés (EFC) et choisir de chiffrer un champ ou une pièce jointe dans une table.

Comment chiffrer les champs

Remarque :
Les champs chiffrés ne sont pas audités par conception. Ce comportement n'est pas configurable.

1. Spécifiez la source de clé : ServiceNow clés générées ou vos clés fournies par le client (apportez votre propre clé) dans **Sécurité de système** > **Paramètres de Chiffrement de champ**.
2. Après avoir spécifié la source de clé, créez un module cryptographique ou utilisez un module cryptographique existant. Commencez par Créer un module cryptographique pour obtenir des instructions.

   Remarque :
   Si vous utilisez des clés fournies par le client, suivez les instructions dans Créer un module cryptographique pour Chiffrement de champ et Configurer les propriétés des clés fournies par le client.

3. Créez une configuration de champs chiffrés pour définir l'endroit où le chiffrement est appliqué. Ici, vous spécifiez la table cible et choisissez de chiffrer ou non une colonne ou des pièces jointes dans la table. Voir Définir des configurations de champs chiffrés pour commencer.

Remarque :
Voir Chiffrement de champ Enterprise Exemples qui illustre comment chiffrer les champs et les pièces jointes à l'aide de clés fournies par le client.

Définir des configurations de champs chiffrés

Configurez les colonnes de table ou les pièces jointes que le système chiffre à l'aide d'un module de chiffrement préconfiguré.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager et security_admin ou élever le rôle à celui d'administrateur de sécurité.

Pourquoi et quand exécuter cette tâche
Assurez-vous d'être dans le périmètre correct de l'application afin de pouvoir afficher les tables dans ce périmètre.

Seuls les utilisateurs ayant accès au module de chiffrement utilisé dans cette configuration peuvent lire les données dans la colonne de table chiffrée ou accéder à la pièce jointe.

- Si un utilisateur dispose d'un accès en écriture, mais pas en lecture, le champ s'affiche en mode d'édition et les données saisies s'affichent sous forme d'astérisques.
- Si un utilisateur dispose d'un accès en lecture mais pas en écriture, le champ affiche les données déchiffrées en mode lecture seule.
- Si un utilisateur dispose de tous les accès, les deux fonctionnalités de lecture/écriture sont disponibles dans le champ chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voir Créer un module cryptographique ou Créer un module cryptographique pour Chiffrement de champ pour commencer.

Important :

Après le chiffrement d'une colonne, toutes les nouvelles données insérées dans la colonne sont chiffrées automatiquement. Toutefois, les données qui existaient dans la colonne avant l'activation du chiffrement ne sont pas automatiquement chiffrées.

Pour chiffrer des données qui existaient avant le chiffrement de la colonne, vous devez exécuter une tâche de chiffrement en masse distincte. Pour en savoir plus sur le chiffrement de masse, consultez Exécuter le chiffrement ou le déchiffrement en masse.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.
2. Sélectionnez **Nouveau**.
3. Renseignez le formulaire.

Champ	Description
Type	**Colonne** pour chiffrer une colonne de table ou **Pièce jointe** pour chiffrer toutes les pièces jointes d'une table. Les types de données chiffrées sont les suivants : ○ Texte de chaîne (UTF-8 complet) ○ Pièces jointes ○ Date, Date/Heure : **Remarque :** Vous pouvez créer des configurations de champs chiffrés pour chiffrer les champs Date et Date/Heure existants. Vous ne pouvez ajouter une nouvelle configuration de chiffrement qu'à une table parente. Vous ne pouvez pas ajouter une nouvelle configuration de chiffrement à une table enfant. ○ URL ○ HTML ○ Journal ○ Traduit
Table	Table dont les champs ou les pièces jointes doivent être chiffrés.
Colonne	Colonne (champ) à chiffrer si vous avez sélectionné **Colonne** comme type.
Actif	Sélectionnez cette option pour marquer la configuration comme active. Désélectionnez si la configuration n'est pas encore utilisée.
Module de chiffrement	Module de chiffrement auquel s'applique la configuration du champ chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fonction de message REST	Sélectionnez **Module unique** pour définir la configuration de champ dans un module. Sélectionnez **plusieurs modules** pour un accès basé sur les rôles qui s'étend sur plusieurs modules cryptographiques. **Module unique** Utilisez cette option pour chiffrer toutes les pièces jointes à l'aide d'un seul module. Vos utilisateurs ont besoin d'accéder à ce module, sinon ils ne sont pas en mesure de charger les pièces jointes. **Modules multiples** Utilisez cette option pour permettre aux utilisateurs de choisir un module lors du chargement des pièces jointes. Les utilisateurs ayant accès à au moins un module peuvent sélectionner un module à utiliser pour le chiffrement. Les utilisateurs n'ayant pas accès au module peuvent charger des pièces jointes non chiffrées.
Conservation chiffrée de l'algorithme [lecture seule]	Indique si le module de chiffrement que vous avez sélectionné est déjà configuré pour prendre en charge le chiffrement non déterministe. Cela signifie que si les mêmes données sont chiffrées plus d'une fois, le chiffrement est différent à chaque fois.

4. Sélectionnez **Soumettre**.

Accès aux scripts pour les modules de chiffrement

Des scripts peuvent être exécutés pour accéder à une politique de module cryptographique à des fins cryptographiques.

Pour Cadre de travail de gestion des clés, les politiques peuvent être basées sur des scripts. Lorsqu'une politique d'accès est déclenchée pour l'accès aux scripts, le script principal peut exécuter les actions de politique du module à partir du script.

Les modules cryptographiques peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement asymétrique des données et le déchiffrement symétrique des données. Chaque objectif cryptographique nécessite la génération d'une clé de chiffrement et un objectif cryptographique défini.

Lors de l'exécution d'une demande de script de chiffrement, tenez compte des points suivants :

- La finalité cryptographique référencée doit être définie dans le module cryptographique.
- Une clé générée active doit exister pour le module de chiffrement.
- Le type de politique d'accès au module doit être défini sur **script**.

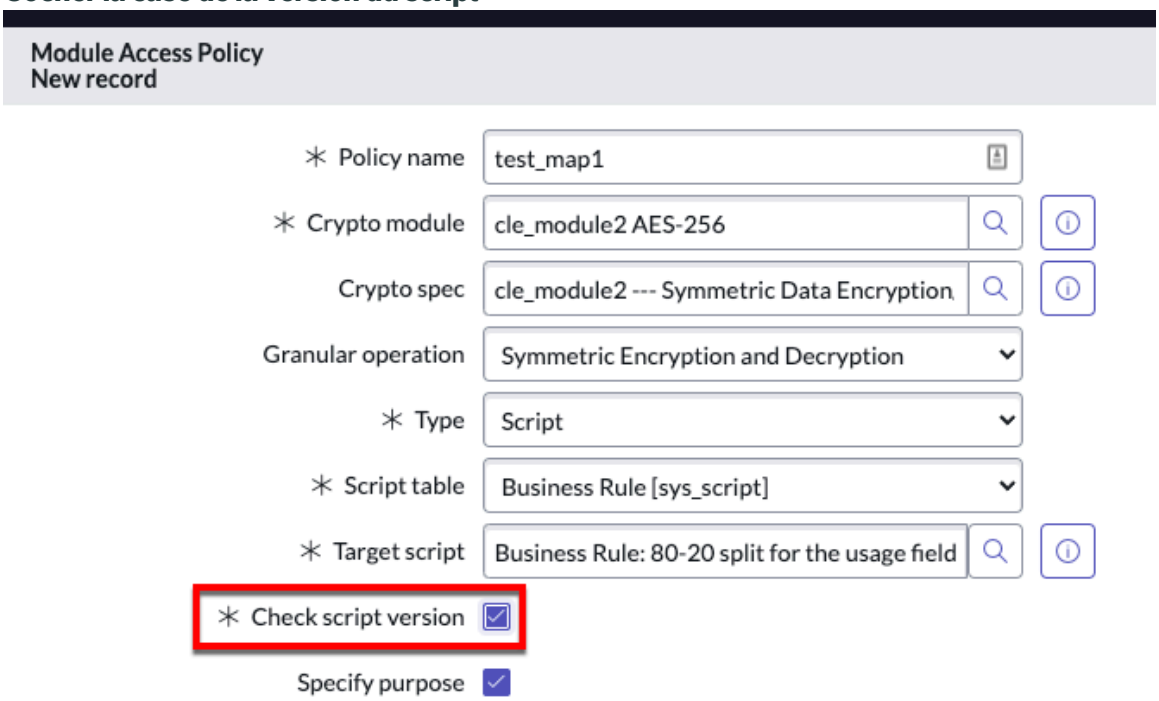
Vérifier la version du script

Lors de la création d'une politique d'accès au module définie sur le type de script, une option permettant de valider l'intégrité de la version de script accessible. Seule la version affectée du script est autorisée à accéder aux modules de chiffrement. Lorsque la case **Vérifier la version du script** est cochée dans la politique d'accès au module, chaque fois que le script est exécuté, le système effectue une comparaison de version. Si le script a été modifié, l'utilisateur en est informé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cocher la case de la version du script



Configurer l'accès des scripts aux données chiffrées

Exécutez un script pour exécuter la politique du module de chiffrement à des fins de chiffrement. Un accès spécifique en lecture (déchiffrer/désencapsuler) ou en écriture (chiffrer, envelopper) peut être défini en fonction de la granularité des opérations de la politique d'accès au module.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

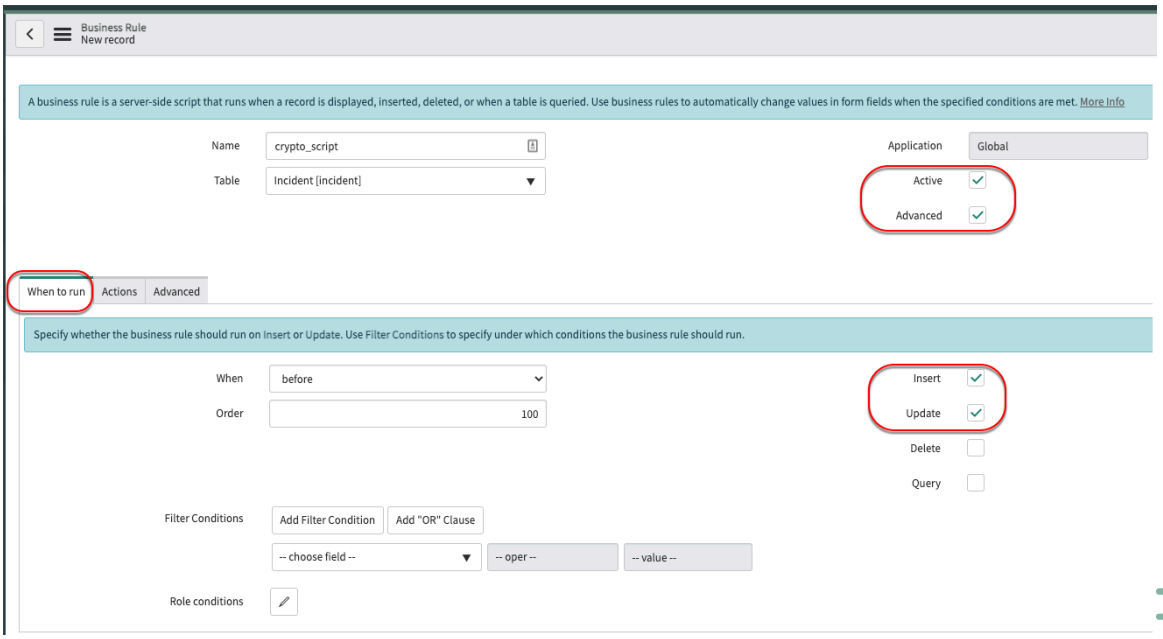
Les règles métier et Includes de script sont des exemples d'utilisations. Cette procédure utilise un script pour les règles métier.

Procédure

1. Créez un module cryptographique avec l'algorithme de chiffrement/déchiffrement de données symétriques. Consultez Créer un module cryptographique pour plus de détails. L'accès spécifique aux données ou à la pièce jointe est contrôlé par une politique d'accès au module présentant les caractéristiques suivantes :
   - Chiffrement symétrique : le script est capable de chiffrer les données, mais ne peut pas les déchiffrer.
   - Déchiffrement symétrique : le script est capable de déchiffrer les données ou les pièces jointes chiffrées chargées, mais il ne peut pas chiffrer les données ou les pièces jointes.
   - Chiffrement et déchiffrement symétriques : le script est capable de chiffrer et de déchiffrer des données ou des pièces jointes.
2. Accédez à la **Définition du système** > **Règles métier**.
3. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Remplissez le formulaire dans l'onglet **Quand exécuter** et entrez le script dans l'onglet **Avancé** :

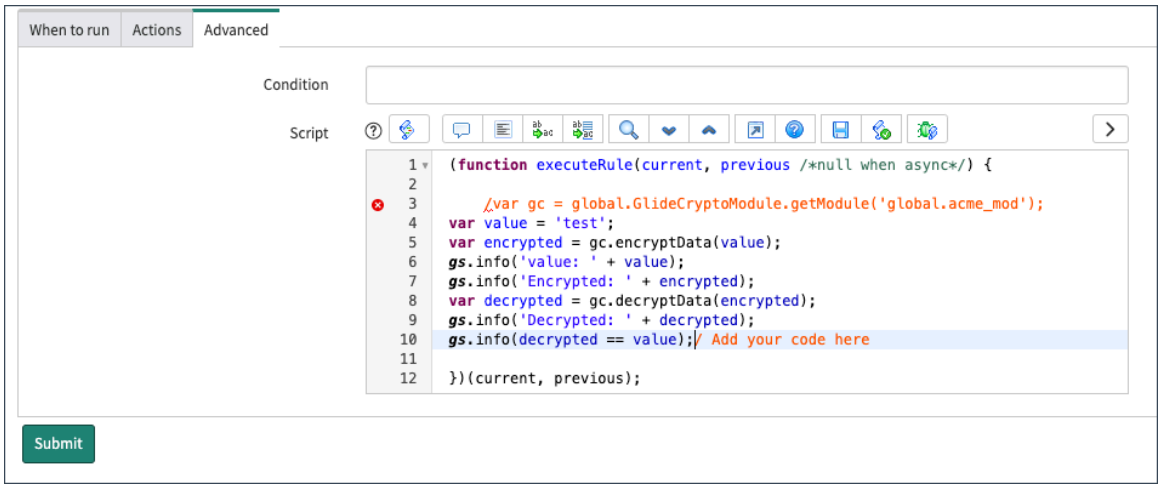
Champs Règle métier

Champ	Description
Nom	Entrez un nom pour la règle métier.
Table	Sélectionnez **Incident [incident]**dans la liste déroulante.
Application	**Global** est sélectionné par défaut.
Actif	Marquez la règle comme **active.**
Avancés	Cochez cette case pour afficher les options avancées.
Onglet Quand exécuter	Dans l'onglet **Quand exécuter** , activez les champs **Insérer** et **Mettre à jour** .

Onglet Avancé	Dans l'onglet **Avancé** , collez le texte de script suivant à la ligne 3 :
	`//`
	`var gc =`
	`global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Remarque : Reportez-vous à l'image « Onglet « Règles métier avancées » pour plus d'informations.

Traduction automatique

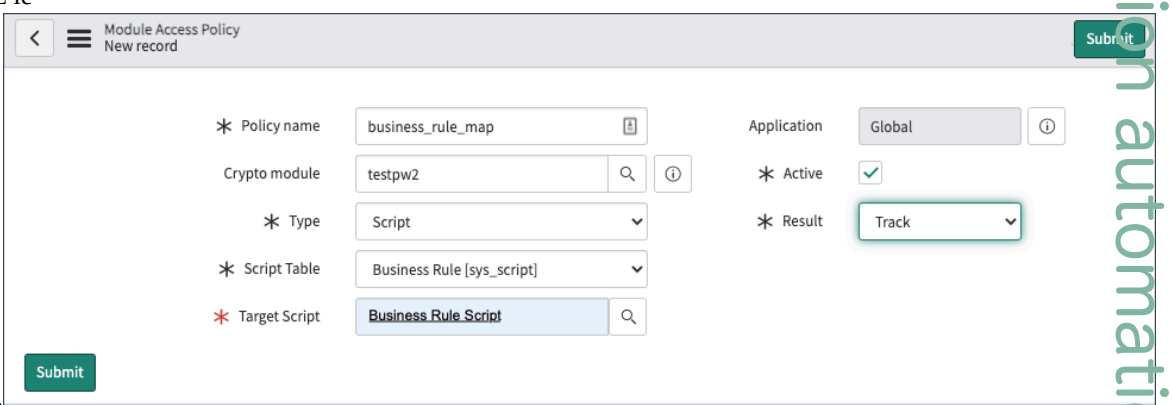
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
6. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.

> **Remarque :**
> Pour plus d'informations, reportez-vous à .Créer une politique d'accès au module

7. Cliquez sur **Nouveau**.
8. Renseignez le formulaire.



Champs de politiques d'accès au module

Champ	Description
Nom de la politique	Saisissez un nom pour la politique.
Module de chiffrement	Cliquez sur l'icône de recherche pour sélectionner un module avec l'algorithme de chiffrement/déchiffrement de données symétriques.
Type	Sélectionnez **Script** pour contrôler l'accès par script.
Table de scripts	Sélectionnez une valeur dans la liste déroulante de la table de scripts. Pour cet exemple, sélectionnez **Règle métier [sys_script].**
Script cible	Sélectionnez le document de script pour la politique. Sélectionnez le **nom** de la table, puis le document

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	connexe pour la politique. Pour cet exemple, sélectionnez la règle métier que vous avez créée lors des étapes précédentes.
Actif	Sélectionnez cette option pour activer la politique.
Résultat	Pour donner au script l'accès au module, sélectionnez **Suivre** dans le champ **Résultat** .

9. Cliquez sur **Envoyer**.
   La politique d'accès au module pour le script est maintenant disponible dans le système.

Afficher les demandes d'utilisation de module de chiffrement refusées

Affichez les modules de chiffrement qui ont rejeté les demandes de chiffrement effectuées par les scripts en raison de mécanismes de chiffrement non pris en charge.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche
Les modules cryptographiques peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement asymétrique des données et le déchiffrement symétrique des données. Les données chiffrées ne sont accessibles qu'en fonction de la politique d'accès au module. Si un script tente d'utiliser un module cryptographique à des fins non définies dans le module, le script ne peut pas accéder aux données chiffrées.

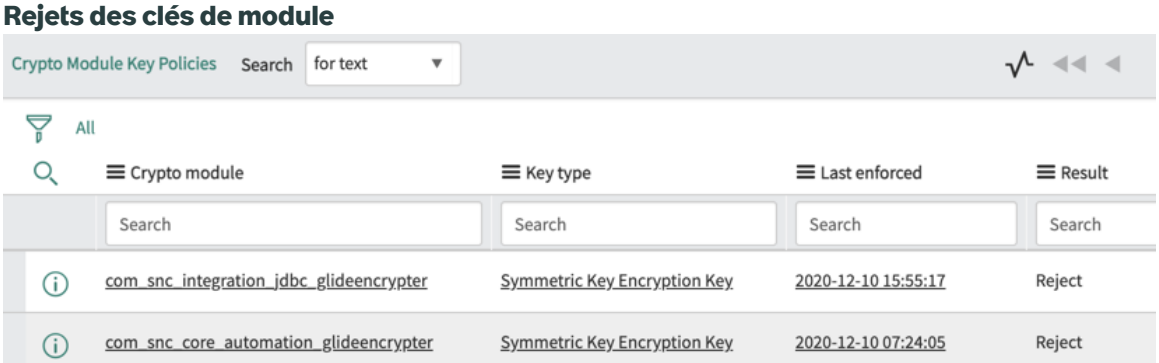
Dans l'exemple suivant, une fonction cryptographique a été affectée à un module cryptographique, mais aucune clé n'a jamais été générée pour cela.

Procédure

Accédez à la **Tous** > **Gestion des clés** > **Politiques de clé de module** > **Rejets des clés de module**.

La liste des modules de chiffrement qui ont rejeté les demandes s'affiche ainsi que la clé de chiffrement utilisée dans le script correspondant.

Rejets des clés de module



Remarque :
Si un script différent tente d'utiliser le même module de chiffrement à l'aide du même type de clé, la valeur pour **Dernières mises à jour appliquées** . Une autre ligne n'est pas générée.

Dans cet exemple, à 2020-02-10_15:55:17, le premier module a rejeté une demande, car la clé de module1 est compromise. Le 2020-02-10_07:24:05, le deuxième module a rejeté une demande car la clé du deuxième module est suspendue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour accorder aux scripts l'autorisation d'utiliser le module de chiffrement lors de leur prochaine exécution, créez une politique d'accès au module pour le chiffrement de script. Pour plus d'informations, référez-vous à Configurer l'accès des scripts aux données chiffrées.

Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse

Planifiez l'exécution des tâches de chiffrement, de déchiffrement et de nouvelle saisie au moment le plus approprié pour vous.

Avant de commencer

Les tâches de chiffrement, de déchiffrement et de nouvelle saisie peuvent demander beaucoup de temps et de ressources, envisagez donc de planifier pendant des heures calmes. Assurez-vous également que l'utilisateur qui planifie la tâche dispose de l'accès approprié pour chaque tâche.

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Le chiffrement et le déchiffrement en masse sont également disponibles à partir du formulaire Configurations de champs chiffrés. Consultez les Exécuter le chiffrement ou le déchiffrement en masse pour obtenir les instructions.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Sécurité**.
2. Cliquez sur **Nouveau**.
3. Remplissez le formulaire de planification.

Champ	Description
Nom	Nom de la tâche de chiffrement, de déchiffrement ou de nouvelle saisie.
Type	Type de tâche : ○ **Contexte de migration clé vers module :** Migration en masse des clés de contexte de chiffrement vers les modules de chiffrement, y compris la création d'enregistrements de politiques d'accès au module pour les contrôles d'accès sur les modules de chiffrement ○ **Contexte de migration des données vers le module** : migre les données chiffrées par contextes de chiffrement vers les modules de chiffrement ○ **Déchiffrement en masse de la pièce jointe**:D chiffre toutes les pièces jointes chiffrées dans les enregistrements d'une seule table que vous définissez dans le champ **Table** . ○ **Chiffrement en masse des pièces jointes** : chiffre toutes les pièces jointes des enregistrements d'une seule table que vous définissez dans le champ **Table** . ○ **Chiffrement en masse** : chiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ ○ **Module de déchiffrement en masse** : déchiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ avec module unique. ○ **Déchiffrement en masse multi-module** : déchiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ avec module multiple.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Renouvellement de saisie en masse** : chiffre à nouveau toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ à l'aide de la clé active actuelle pour le module. ○ **Migrer le contexte de la pièce jointe vers le module** : chiffre toute pièce jointe préexistante dans la table définie dans la configuration de chiffrement de champ. Toute pièce jointe précédemment chiffrée avec un contexte est à nouveau chiffrée avec le module.
État	L'état initial de la tâche est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état est mis à jour en conséquence.
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures.
Fin de la fenêtre de temps	Heure de fin de la tâche au format 24 heures.
Table	Table à chiffrer ou à déchiffrer.
Champ	Champ à chiffrer ou à déchiffrer.
Résumé	Informations sur l'état d'une tâche lorsque la tâche est en cours d'exécution, est terminée ou présente des erreurs.

Remarque :
En raison de la surcharge système, vous devez planifier l'exécution des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse en dehors des heures de pointe. Exécute ServiceNow AI Platform la tâche entre le **début** et la fin de la **fenêtre de temps**. Si la tâche n'est pas terminée dans une fenêtre de traitement, elle se poursuit pendant la fenêtre de traitement spécifiée suivante jusqu'à ce que tout le traitement soit terminé.

4. Cliquez sur **Envoyer**.
5. Après avoir planifié une tâche, vous pouvez effectuer les opérations suivantes.
   - Cliquez sur **Annuler la tâche** pour annuler une tâche en cours d'exécution.
   - Cliquez sur **Démarrer** pour démarrer une tâche immédiatement.
   - Cliquez sur **Mettre à jour** pour enregistrer les modifications que vous apportez au calendrier de tâche.
   - Cliquez sur **Supprimer** pour supprimer la tâche planifiée.

Exécuter le chiffrement ou le déchiffrement en masse

Vous pouvez exécuter le chiffrement en masse sur les configurations de chiffrement, ainsi qu'un déchiffrement en masse pour déchiffrer les valeurs précédemment chiffrées.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez également créer des travaux planifiés pour le chiffrement et le déchiffrement en masse. Consultez les Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse pour obtenir les instructions.

Le chiffrement et le déchiffrement en masse ne sont disponibles que lorsqu'une configuration de champ chiffré utilise le module de chiffrement unique. Le déchiffrement en masse est disponible pour la méthode de chiffrement unique et multiple.

Remarque :
Vous devez exécuter le chiffrement et le déchiffrement en masse uniquement en dehors des heures de pointe, car les opérations sont gourmandes en ressources et en temps.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.
2. Ouvrez la configuration des champs chiffrés pour le champ que vous souhaitez chiffrer ou déchiffrer en masse.
3. Sous Liens connexes, sélectionnez une option disponible.
   - **Planifier la tâche de déchiffrement en masse**
   - **Planifier la tâche de chiffrement en masse**
4. Confirmez votre sélection dans la boîte de dialogue.

Résultats

En cas d'exécution d'un chiffrement en masse, toutes les valeurs sont chiffrées avec le module de chiffrement défini dans l'enregistrement de configuration du champ chiffré. Si vous exécutez un déchiffrement en masse, seuls les champs chiffrés avec un module de chiffrement auquel vous avez accès sont déchiffrés.

Télécharger les pièces jointes pour chiffrement

Protégez les fichiers sensibles en chiffrant les pièces jointes des enregistrements à l'aide du chiffrement de champ et des conditions de ligne.

Avant de commencer

Rôle requis : tout rôle qui s'aligne sur la politique d'accès au module (MAP) créée par l'administrateur.

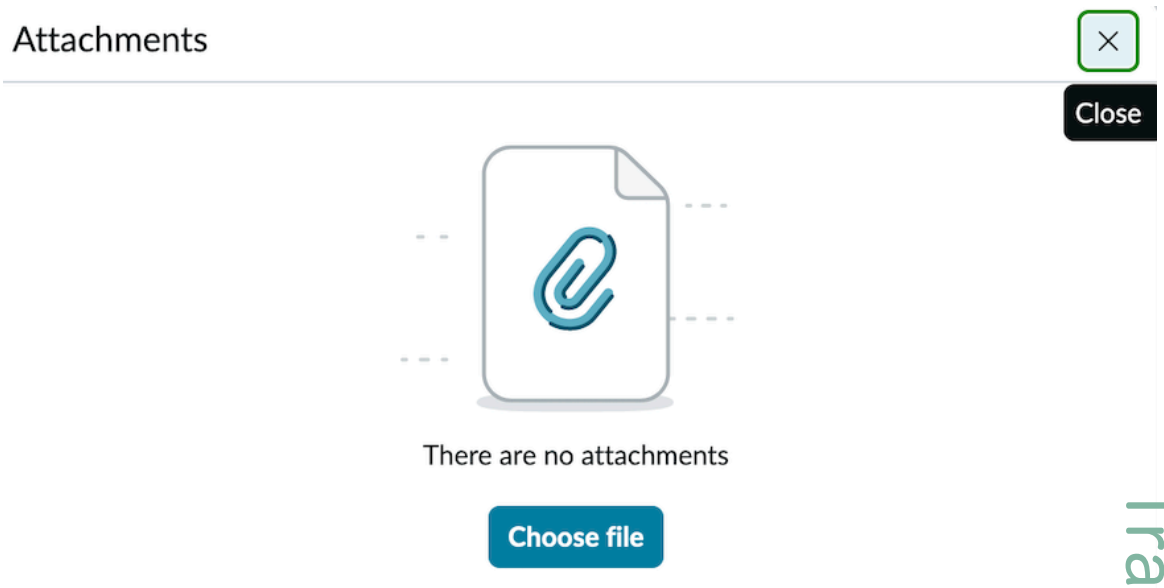
Procédure

1. Accédez à un enregistrement.
2. Sélectionnez l'icône **Trombone Gérer les pièces jointes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la fenêtre **Pièces jointes** , sélectionnez le module à chiffrer dans les options déroulantes **Chiffrer avec**



module .



Remarque :

Si des conditions de ligne ont été ajoutées à la configuration du champ de chiffrement, cette option ne s'affiche pas. La pièce jointe serait alors automatiquement chiffrée avec le module défini dans la condition de ligne. De même, cette option de liste déroulante ne s'affiche que lors de l'utilisation de l'icône Gérer les pièces jointes et non si la pièce jointe est ajoutée par glisser-déplacer.

4. Sélectionnez **Choisir un fichier** pour localiser la pièce jointe et sélectionnez **Ouvrir** pour la joindre.

Résultats
Les fichiers joints s'affichent en haut du formulaire. Les pièces jointes chiffrées sont indiquées par un verrou. Seuls les utilisateurs disposant du module de chiffrement permettant d'afficher les fichiers chiffrés les verront dans la liste.

Chiffrement de champ Enterprise Exemples

Ces exemples vous guident dans le chiffrement des champs et des pièces jointes à l'aide de clés fournies par le client.

Chiffrement de champ Enterprise Procédure pas à pas

Cette procédure pas à pas vous montre comment chiffrer un champ dans votre instance à l'aide Chiffrement de champ Enterprise de Cadre de travail de gestion des clés (KMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure ne s'applique qu'aux Chiffrement de champ Enterprise fonctionnalités. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : admin ou security_admin

Remarque :
security_admin s'agit d'un rôle privilégié, pour plus de détails sur l'utilisation des rôles privilégiés, voir Élever à un rôle privilégié

Pourquoi et quand exécuter cette tâche

Cette procédure pas à pas commence par une instance dans laquelle vous avez déjà créé et chargé votre clé cryptographique personnelle. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le ServiceNow client.

Une fois la clé stockée dans un module cryptographique, vous pouvez commencer à configurer des champs dans votre instance, tels que les numéros de salaire ou de sécurité sociale dont l'accès de certains utilisateurs est limité. Dans la configuration des champs chiffrés, spécifiez le personnel autorisé qui peut accéder aux données sensibles.

Cette tâche présente deux scénarios. Par exemple, le champ **Brève description** d'un incident est chiffré pour les utilisateurs qui ne sont pas autorisés à afficher les données sensibles.

Les pièces jointes peuvent également être chiffrées et visibles uniquement par les utilisateurs qui y ont accès, ou par tous les utilisateurs qui ne sont pas autorisés à consulter les données. Voir Procédure pas à pas avec chiffrement de pièce jointe pour chiffrer une pièce jointe.

Procédure

1. Assurez-vous que cette Chiffrement de champ Enterprise option est activée.
2. Créez un module cryptographique pour column_level_encryption.
   Consultez la section Créer un module cryptographique pour Chiffrement de champ Créer un module cryptographique pour plus d'informations.
3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Remplissez les champs du formulaire.

Formulaire Configuration des champs chiffrés

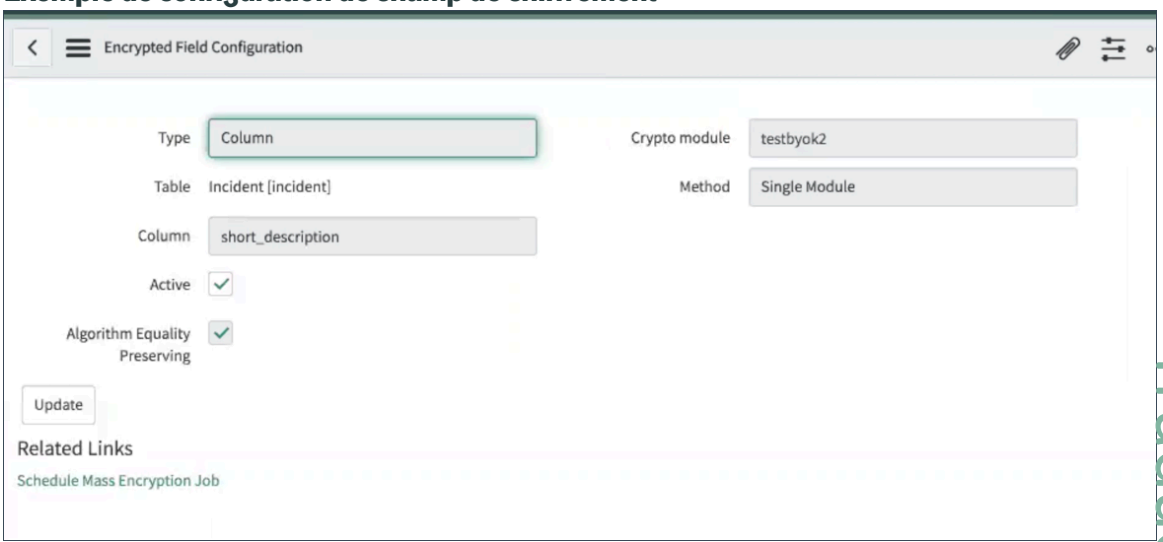
Champ	Description
Type	**La colonne** est requise pour utiliser votre clé personnelle.
Table	Table qui stocke les informations sensibles. Pour cet exemple, sélectionnez **Incident [incident].**
Colonne	Colonne ou informations spécifiques qui représentent la date sensible à chiffrer. Pour cet exemple, sélectionnez **short_description**.
Actif	Option permettant de marquer **comme actif** pour utiliser la configuration du champ.
Préservation de l'égalité d'algorithme	L'option est automatiquement sélectionnée.
Module de chiffrement	Module que vous avez créé pour l'utiliser avec la clé personnelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fonction de message REST	L'option **Module unique** permet d'appliquer les politiques pour un module. **Plusieurs modules** permet d'appliquer les politiques à plusieurs modules.

Exemple de configuration de champ de chiffrement



6. Cliquez sur **Envoyer**.

Établissez une politique d'accès au module pour affecter l'accès au module cryptographique. Consultez Créer une politique d'accès au module pour plus d'informations.

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > > **Créer** > **.**
8. Remplissez les champs du formulaire.

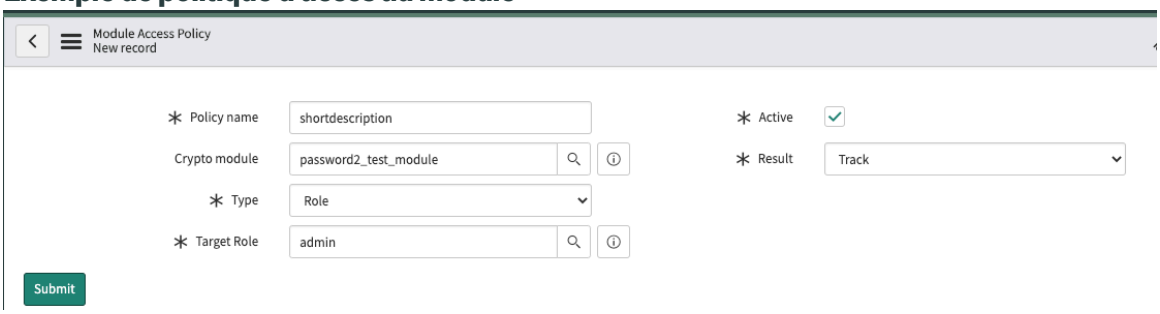
Formulaire de politique d'accès au module

Champ	Description
Nom de la politique	Nom de la politique, par exemple description brève.
Module de chiffrement	Module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Type de désignation d'accès pour la politique de chiffrement. Utilisez **Rôle** pour accorder l'accès au champ chiffré uniquement aux utilisateurs qui ont le rôle affecté.
Rôle cible	Le rôle qui a accès au champ chiffré. Pour cet exemple, sélectionnez **Administrateur**.
Actif	Option permettant d'activer la politique d'accès au module.
Résultat	L'option **Suivre**active l'accès au champ pour le rôle sélectionné. (Pour restreindre l'accès à ce champ au rôle sélectionné, sélectionnez **Rejeter** ou**Rejeter strictement**.)

Traduction automatique

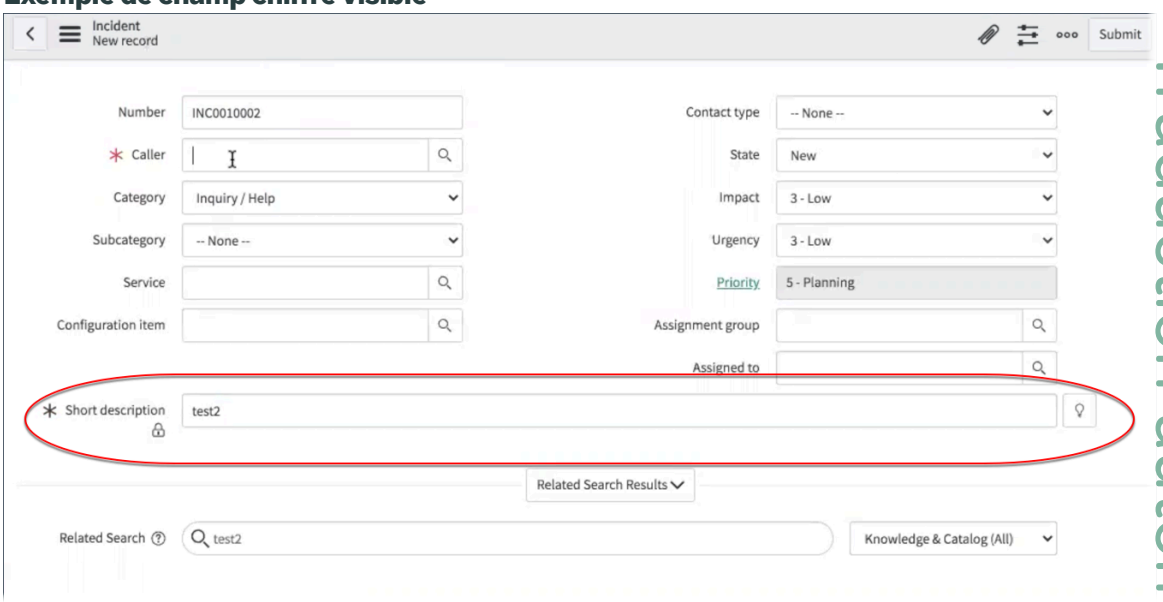
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de politique d'accès au module



9. Cliquez sur **Envoyer**.
10. En tant qu'utilisateur disposant du rôle sn_kmf.admin, accédez à **Incident** > **Nouveau**.

Exemple de champ chiffré visible



Vous pouvez maintenant afficher le champ Description brève en fonction de la configuration de la politique d'accès au module.

Remarque :
Le rôle sn_kmf.admin a reçu l'accès utilisateur au champ chiffré, Brève description, en définissant la politique d'accès au module sur **Suivre**. L'icône de verrouillage ( ) sous le nom du champ indique que le champ est un champ chiffré.

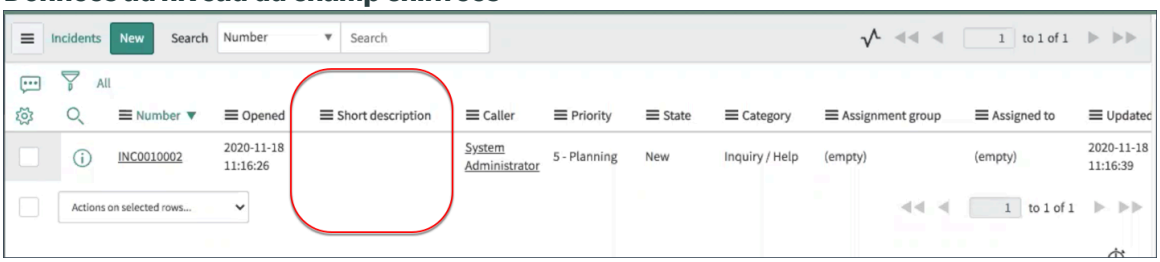
Vous pouvez maintenant accéder au module **Incidents** en tant qu'utilisateur final pour tester la configuration des champs chiffrés.

11. Connectez-vous en tant qu'utilisateur pour ne pas pouvoir afficher les données chiffrées dans le champ configuré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Données au niveau du champ chiffrées



Lorsque vous accédez au numéro d'incident, les données de la brève description ne sont pas visibles.

Résultats

Vous avez utilisé avec succès votre clé symétrique pour contrôler l'accès à un champ spécifique à l'aide de Chiffrement de champ Enterprise.

Procédure pas à pas avec chiffrement de pièce jointe

Cette procédure pas à pas vous montre comment chiffrer une pièce jointe dans votre instance à l'aide Chiffrement de champ Enterprise du Cadre de travail de gestion des clés (KMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure ne s'applique qu'aux Chiffrement de champ Enterprise fonctionnalités. Voir Activer Chiffrement de champ pour plus d'informations sur l'obtention Chiffrement de champ Enterprise de .

Rôle requis : gestionnaire de chiffrement kmf

Pourquoi et quand exécuter cette tâche

Cette procédure pas à pas commence par une instance dans laquelle vous avez déjà créé et téléchargé la clé cryptographique fournie par le client. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le client.

Téléchargez des pièces jointes confidentielles dans votre instance et limitez l'accès de certains utilisateurs. Utilisez la configuration des champs chiffrés pour spécifier quel personnel autorisé peut accéder aux données sensibles.

Nous vous montrons comment chiffrer les pièces jointes pour qu'elles ne soient visibles que par les utilisateurs auxquels l'accès est accordé, ou pour tous les utilisateurs qui ne sont pas autorisés à consulter les données. Dans cet exemple, nous limitons l'accès à une pièce jointe dans le module **Incidents** pour un certain rôle.

Remarque :
Bien que vous puissiez utiliser plusieurs modules avec Chiffrement de champ Enterprise, le chiffrement de la pièce jointe doit utiliser des modules uniques.

Procédure

1. Assurez-vous que cette Chiffrement de champ Enterprise option est activée.
2. Créez un module cryptographique.
   Consultez Créer un module cryptographique pour Chiffrement de champ pour plus d'informations.
3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Remplissez le formulaire :

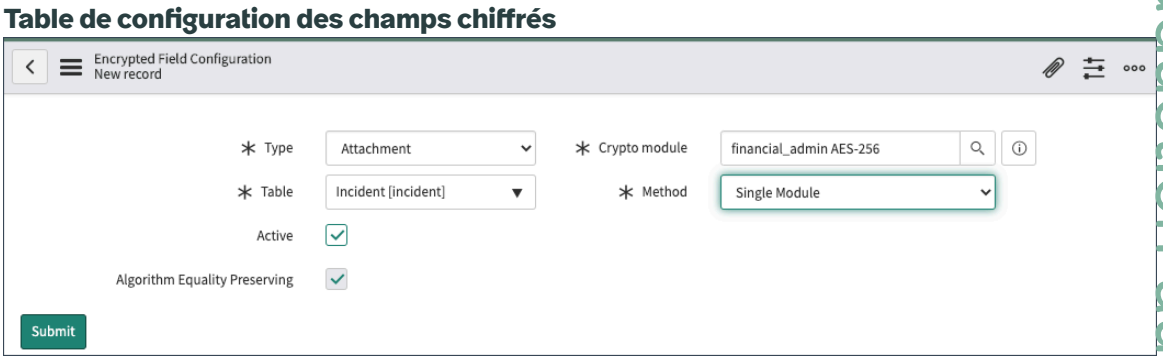
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de configuration des champs chiffrés

Champ	Description
Type	Sélectionnez **Pièce jointe** pour utiliser votre clé personnelle pour chiffrer une pièce jointe de la **table** sélectionnée Pour cet exemple, sélectionnez **Incident**.
Table	Sélectionnez la table pour accéder aux informations sensibles. Pour cet exemple, sélectionnez **Incident [incident].**
Actif	Marquez **comme actif** pour pouvoir utiliser la configuration du champ.
Préservation de l'égalité d'algorithme	Lorsque vous sélectionnez Chiffrement de champ Enterprise, ce champ est visible en fonction de la table sélectionnée.
Module de chiffrement	Sélectionnez le module que vous avez créé pour l'utiliser avec la clé personnelle.
Fonction de message REST	L'option **Module unique** permet d'appliquer les politiques pour un module. **Plusieurs modules** permet d'appliquer les politiques à plusieurs modules.

Table de configuration des champs chiffrés



6. Cliquez sur **Envoyer**.

Établissez une politique d'accès au module pour affecter l'accès au module cryptographique. Reportez-vous à pour plus d'informations Créer une politique d'accès au module .

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
8. Cliquez sur **Nouveau**.
9. Remplissez le formulaire :

Champs de politique d'accès au module

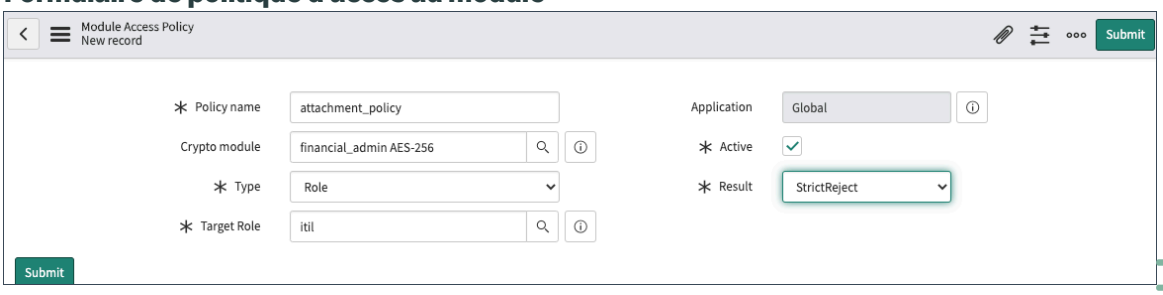
Champ	Description
Nom de la politique	Saisissez un nom pour la politique, par exemple « Politique des pièces jointes ».
Module de chiffrement	Sélectionnez le module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Sélectionnez **Rôle** pour restreindre l'accès au champ chiffré des utilisateurs disposant du rôle affecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

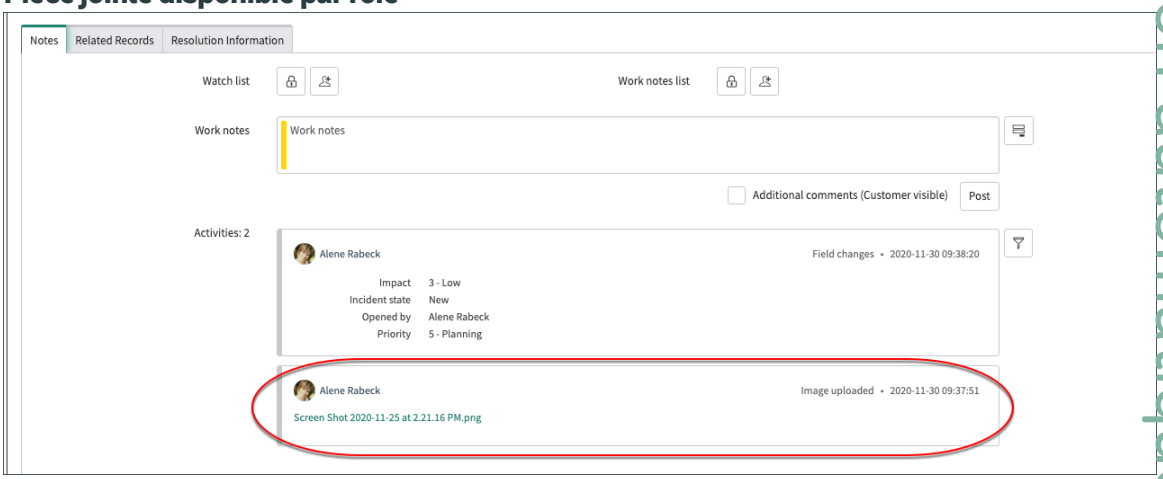
Champ	Description
Rôle cible	Sélectionnez le rôle qui n'aura pas accès au champ chiffré. Pour cet exemple, sélectionnez **itil**.
Actif	Cochez cette case pour pouvoir utiliser la politique d'accès au module.
Résultat	Sélectionnez **Rejeter strictement** pour contrôler l'accès à la pièce jointe à partir du rôle sélectionné. (Pour accorder l'accès au rôle sélectionné, sélectionnez **Suivre**.)

Formulaire de politique d'accès au module



10. Cliquez sur **Envoyer**.
11. En tant qu'administrateur ou personne ayant créé l'incident, accédez à **Incidents** et ajoutez une pièce jointe aux **activités** dans la liste connexe **Notes** .

Pièce jointe disponible par rôle



12. Connectez-vous en tant qu'utilisateur ayant restreint l'accès à la pièce jointe chiffrée.
13. Ouvrez l'incident et accédez à la section **Activités :** .
    Le lien permettant d'ouvrir la pièce jointe n'est pas accessible aux utilisateurs avec le rôle restreint.
14. Vous avez désormais utilisé avec succès la clé fournie par le client pour contrôler l'accès à une pièce jointe spécifique à l'aide Chiffrement de champ Enterprise de .

Chiffrement de champ Enterprise

Chiffrement de champ Enterprise utilise le Cadre de travail de gestion des clés (KMF) pour vous permettre de personnaliser et de gérer la façon dont les champs et les pièces jointes sont chiffrés et déchiffrés sur votre instance. Un abonnement est requis pour utiliser Chiffrement de champ Enterprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
Cette rubrique couvre la version entreprise de Chiffrement de champ. Pour plus d'informations sur la version standard de Chiffrement de champ ou pour connaître les différences entre les deux versions, reportez-vous à la section Explorer Chiffrement de champ.

Chiffrement de champ Enterprise est basé avec Chiffrement de champ et utilise le et sa prise en charge complète des fonctions de gestion des clés. Chiffrement de champ Enterprise assure la protection des clés et la gestion du cycle de vie des clés pour le Cadre de travail de gestion des clés chiffrement des champs au niveau de l'application. Toutes les clés sont protégées par une hiérarchie d'encapsulation de clés ancrée dans les modules de sécurité matériels (HSM) FIPS (Federal Information Processing Standards) 140-2-L3.

Chiffrement de champ Enterprise vous donne la possibilité de gérer la façon dont les champs pris en charge sont chiffrés et déchiffrés conformément aux pratiques de la norme NIST 800-57 . Il utilise également la version la plus récente du chiffrement au niveau des champs, y compris l'intégration pour une protection et une gestion appropriées des clés.

Plus précisément, Chiffrement de champ Enterprise utilise les modules de chiffrement, ce qui vous accorde plus de contrôle sur le chiffrement côté serveur. KMF Vérifie la protection appropriée des clés de chiffrement des données à l'aide de la KMF hiérarchie de clés et du chiffrement d'enveloppe. Votre instance chiffre les données via des modules de chiffrement que vous configurez. Vous pouvez créer une politique d'accès pour chaque module, puis configurer des spécifications cryptographiques et des politiques d'accès et contrôler le contrôle de la gestion du cycle de vie des clés.

Chiffrement de champ Enterprise Prend en charge les politiques d'accès au module basées sur :

- Champ d'application
- Rôle
- Script
- Échange de ressources
- Utilisateur système

Consultez Créer une politique d'accès au module pour plus d'informations.

Remarque :
Pour plus de détails sur les fonctionnalités prises en charge et sur la manière de Chiffrement de champ mettre à niveau et de s'abonner à l'autorisationChiffrement de champ Enterprise, reportez-vous à .Chiffrement et gestion des clés par lot

Conditions de chiffrement

Terme	Description
Gestion des clés 	Prise en charge de la gestion des clés Le cadre de gestion des clés (KMF) est fondamental Chiffrement de champ Enterprise . Bénéficiez des options suivantes : • Gestion du cycle de vie des clés. • Rotation de clés. Consultez Faire pivoter les clés pour en savoir plus.

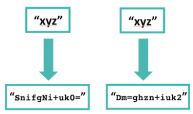
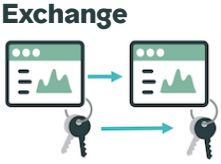
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Terme	Description
	• Protection et génération de clés avec les modules de sécurité matériels (HSM) FIPS 140-2-L3. • Séparation des rôles et des tâches. • Le transfert sécurisé des clés de chiffrement des données entre les instances, telles que les instances de production et de non-production. • Clés fournies par le client (CSK) avec emballage de clé. • Chiffrement non déterministe. • Chiffrement/déchiffrement en masse. • Audit de l'accès et de l'utilisation des clés. Consultez Référence du cadre de travail de gestion des clés pour en savoir plus.
Clé fournie par le client 	Prise en charge des clés fournies par le client L'un des plus grands avantages Chiffrement de champ Enterprise est que vous pouvez utiliser vos propres clés pour le cryptage. Les administrateurs ont le choix d'utiliser ServiceNow les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur le ServiceNow AI Platform®. Vous pouvez également gérer le cycle de vie des clés et décider quand révoquer, faire pivoter et désactiver les clés. Une fois que vous avez activé les clés fournies par le client et créé un module cryptographique, vous téléchargez un jeton et une clé éphémère publique. Vous utilisez le jeton et la clé publique pour encapsuler votre clé, puis la charger dans l'instance. Pour utiliser les clés fournies par le client, reportez-vous aux sections Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé et Utilisation des clés fournies par le client avec Chiffrement de champ Enterprise.
Chiffrement de champ 	Prise en charge du chiffrement de champ et du chiffrement des pièces jointes Le chiffrement de champ et le chiffrement de pièce jointe utilisent tous deux des modules cryptographiques et des stratégies d'accès via des configurations de champs chiffrés. Le formulaire Configuration des champs chiffrés est utilisé pour choisir un type de chiffrement de *colonne* ou de *pièce jointe* . Consultez pour Définir des configurations de champs chiffrés plus d'informations et les types de champs pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Terme	Description
Chiffrement non déterministe 	Prise en charge du chiffrement non déterministe Chiffrement de champ Enterprise prend en charge le chiffrement *non déterministe* pour une sécurité renforcée. Si le système crypte les mêmes données plus d'une fois, les textes chiffrés sont différents à chaque fois. Le chiffrement non déterministe est disponible avec le chiffrement AES (Advanced Encryption Standard) avec le chaînage de blocs de chiffrement (CBC). Vous pouvez activer cette fonctionnalité via l'option Préservation de l'égalité à l'étape Définition de l'algorithme de la spécification cryptographique. Créez une spécification cryptographique pour un module de chiffrement et définissez un algorithme pour le chiffrement et générez la clé. Reportez-vous à la section Créer un module cryptographique pour définir les mécanismes utilisés pour les opérations cryptographiques et pour plus d'informations sur l'activation du chiffrement non déterministe.
Resource Exchange 	Resource Exchange Chiffrement de champ Enterprise clés d'instance en instance de manière sécurisée à l'aide d'API cryptographiques pour assurer la confidentialité, l'intégrité KMF , l'authentification et la non-répudiation. Resource Exchange est une KMF fonctionnalité qui vous permet d'échanger des ressources entre les instances de manière sécurisée. Consultez Échange de ressources du cadre de travail de gestion des clés pour en savoir plus.

Remarque :
Si vous choisissez de ne pas activer Chiffrement de champ Enterprise, vous pouvez toujours utiliser Chiffrement de champ. Pour plus d'informations, reportez-vous Explorer Chiffrement de champ à la section .

Chiffrement de champ Enterprise prend en charge les clients sur site. Séparation en domaines n'est pas prise en charge.

Prise en charge de champs chiffrés supplémentaires

La version standard de Chiffrement de champ est limitée à cinq colonnes chiffrées. Chiffrement de champ Enterprise prend en charge un nombre illimité de colonnes chiffrées.

Informations sur les champs pris en charge

Les types de champs suivants peuvent être chiffrés :

- Pièces jointes
- Date
- Date/Heure
- E-mail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- HTML
- Journal
- Entrée de journal
- Liste de journaux
- Téléphone
- Texte de chaîne
- Champ traduit
- HTML traduit
- Texte traduit
- URL

Chiffrement de la pièce jointe

Chiffrement de la pièce jointe par défaut

Les clients utilisant Chiffrement de champ des pièces jointes sont chiffrées par défaut dans des tables dont le type de configuration de champs chiffrés (EFC) actif est *`Attachment`*.

Ce chiffrement par défaut défini par la configuration EFC signifie que les administrateurs n'ont pas besoin de déclarer manuellement qu'une pièce jointe doit être chiffrée au chargement pour ces tables.

Les administrateurs peuvent interdire aux utilisateurs de joindre des fichiers non chiffrés

Pour plus de détails, voir Empêcher les utilisateurs de joindre des fichiers non chiffrés.

Refuser le chiffrement par défaut

Si vous ne souhaitez pas que les pièces jointes soient chiffrées par défaut en fonction de la configuration EFC, vous pouvez désactiver cette option en contactant ServiceNow le support.

Pour vous désabonner de cette fonctionnalité, créez un ticket de support auprès ServiceNow du support et incluez cette déclaration dans un commentaire sur l'enregistrement du ticket :

« Je [nom du client] comprends que je demande ServiceNow de désactiver une bonne pratique de sécurité recommandée pour les pièces jointes et que [l'entreprise cliente] assume tout risque supplémentaire lié à sa configuration et à son utilisation de pièces jointes non chiffrées dans l'application ServiceNow . »

Prise en charge de l'API

Chiffrement de champ Enterprise met à jour les API `setDisplayValue()` et `setValue()` afin qu'elles puissent insérer des données chiffrées pour les champs chiffrés. Il permet également à `getDisplayValue()` et `getValue()` de renvoyer des valeurs en texte clair.

Le script suivant illustre ces changements d'API lorsque la brève description de l'incident est chiffrée :

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Lorsque vous utilisez `getValue()` pour obtenir du texte chiffré, votre script ne renvoie plus le texte chiffré. Votre script renvoie le texte en clair, en supposant que l'utilisateur a accès au module de chiffrement. `getValue()` renvoie le texte chiffré pour les utilisateurs qui n'ont pas accès au module cryptographique.

Chiffrement dans le cloud avec gestion des clés

ServiceNow® Chiffrement dans le cloud offre un stockage chiffré pour la base de données à l'aide du chiffrement de bloc, ainsi qu'une gestion améliorée des clés. Chiffrement dans le cloud est disponible avec le ServiceNow® Lot d'abonnements à Platform Encryption.

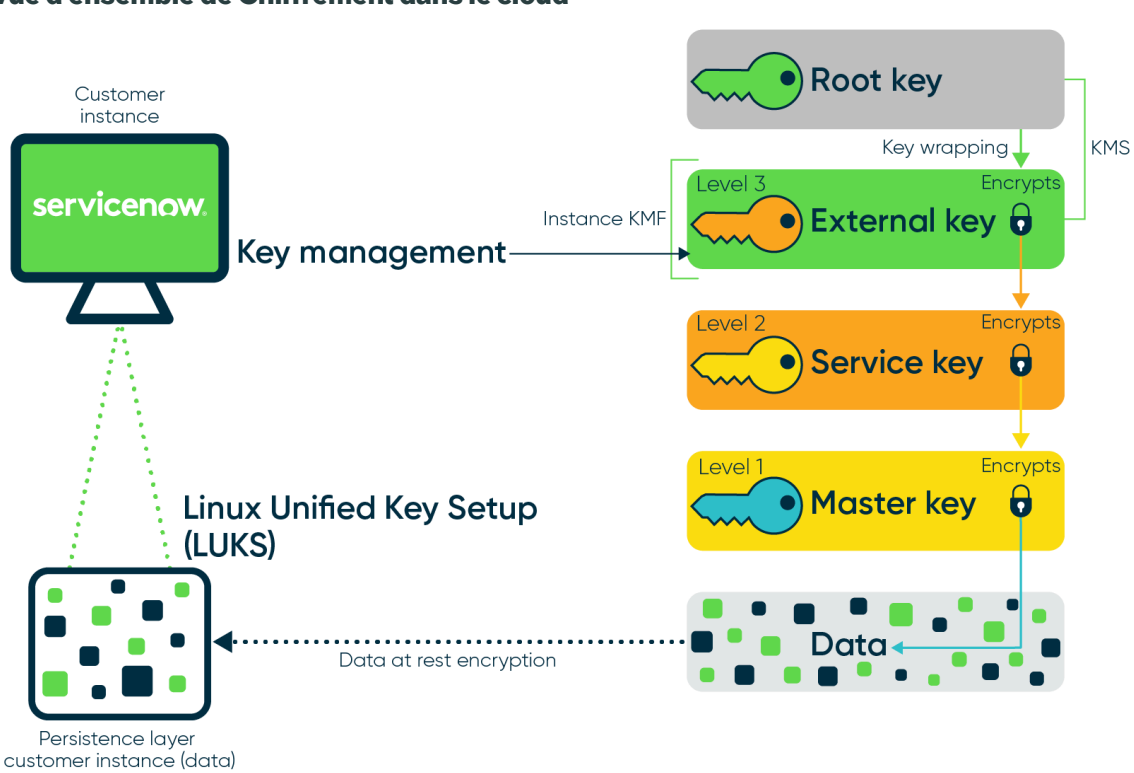
Chiffrement dans le cloud Offre:

- Séparation des tâches.
- Rotation des ServiceNow clés gérées.
- Option Clés gérées par le client.

Remarque :
Envisagez cette option si votre organisation vous demande d'utiliser du matériel de clé généré par vos propres outils ou bibliothèques cryptographiques, un système de gestion des clés d'entreprise ou un module de sécurité matériel (HSM). Consultez Opérations de gestion des clés pour en savoir plus.

Le diagramme suivant montre comment Chiffrement dans le cloud fonctionner.

Vue d'ensemble de Chiffrement dans le cloud



Le Chiffrement dans le cloud module Gestion des clés comprend les sous-modules suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Opérations de gestion des clés:
  - Accédez à la liste des clés.
  - Effectuer des opérations de rotation des clés.
  - Retirer la clé gérée par le client.
- Transactions de gestion des clés:

  Référencez toutes les transactions qui se sont produites pour les clés qui ont été utilisées.

  Utilisez votre propre clé gérée par le client pour le chiffrement.

Dans certaines circonstances, vous pouvez opter pour une demande de retrait de clé lorsque vous utilisez une clé gérée par le client. Pour ce faire, vous devez obtenir une licence pour l'UGS du complément facultatif Retrait et réapprovisionnement de Chiffrement cloud, puis demander à un Service client et assistance membre de l'équipe d'activer la fonctionnalité de retrait de clé.

L'option Paramètres de politique de contrôle du quorum devient disponible lorsque la fonctionnalité de retrait est activée, sinon le module n'est pas visible dans le menu. Cette fonctionnalité ne peut être activée que lors de l'utilisation de clés gérées par le client. Cette politique permet de configurer des paramètres concernant le quorum lorsque la fonctionnalité de retrait est activée. Pour en savoir plus sur cette fonctionnalité, reportez-vous à la section Politique de contrôle du quorum.

Chiffrement dans le cloud prend en charge les instances de production et de non-production pour les bases de données MariaDB et RaptorDB. Cloud Encryption est pris en charge dans le cloud commercial, le pod 101 du cloud pour les clients du gouvernement (GCC) et ServiceNow la ServiceNow plateforme protégée – Australie (SPP-AU).

Gestion des licences et activation Chiffrement dans le cloud

Pour en savoir plus sur la gestion des licences Chiffrement dans le cloud, reportez-vous à la section Chiffrement et gestion des clés par lot.

Pour les clients sous licence avec de nouvelles instances, la mise en service de la nouvelle instance inclura Chiffrement dans le cloud.

Pour les clients sous licence disposant d'instances existantes, pour demander le déplacement d'une instance vers Chiffrement dans le cloud, suivez les instructions de la section KB1117369 . Vous devez avoir le rôle d'administrateur client ou d'administrateur partenaire pour demander l'élément de Catalogue de services afin d'activer Chiffrement dans le cloud sur votre instance. L'activation de cette fonctionnalité nécessite une fenêtre de maintenance d'une heure.

Interface utilisateur de Chiffrement dans le cloud

Lorsque Chiffrement dans le cloud est activé, l'interface utilisateur de Chiffrement dans le cloud est visible par l'utilisateur security_admin lorsque cet utilisateur a le rôle sn_kmf.admin.

Pour accéder à l'interface utilisateur de Chiffrement dans le cloud en recherchant **Gestion de clé de chiffrement dans le cloud** dans la barre de navigation. Accédez à la section **Opérations de gestion des clés** pour afficher des informations sur les clés de chiffrement,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

telles que les détails de la clé active et si Chiffrement dans le cloud est activé pour l'instance.

Opérations de gestion des clés

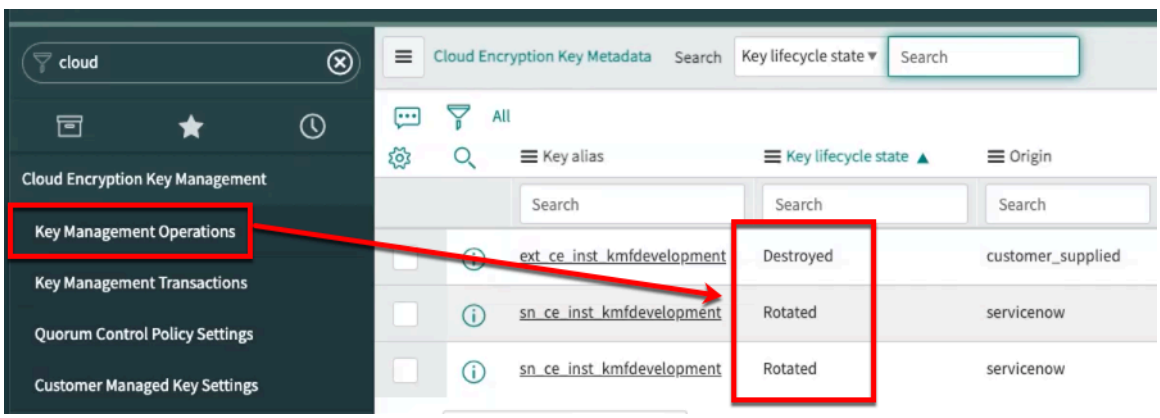
Le sous-module Opérations de gestion des clés permet d'afficher et de gérer toutes les clés de chiffrement utilisées avec ServiceNow Chiffrement dans le cloud.

Mise en route de Chiffrement dans le cloud

États du cycle de vie des clés

Il n'y a qu'une seule clé active dans le système à la fois. Lorsque vous sélectionnez une clé, vous accédez à l'activité de la clé sélectionnée, telle que les clés qui ont été tournées ou retirées et l'horodatage correspondant.

L'état du cycle de vie des clés est mis à jour en fonction de l'opération de gestion des clés effectuée.



Voir Faire pivoter une clé gérée par ServiceNow ou Rotation d'une clé gérée par le client pour plus de détails.

Remarque :
Le processus de rotation de clés peut prendre jusqu'à 20 minutes.

Faire pivoter une clé gérée par ServiceNow

Faites pivoter la clé gérée active Chiffrement dans le cloud ServiceNow .

Avant de commencer
Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Important :
Si vous utilisez des clés gérées par le client, reportez-vous à la section Rotation d'une clé gérée par le client.

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
   La Chiffrement dans le cloud liste des métadonnées clés se charge. Toutes les clés utilisées dans votre instance sont répertoriées. Une seule clé peut être active à la fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous accédez au module pour la Chiffrement dans le cloud première fois, les entrées de clés seront disponibles après une première rotation de clés. Une ServiceNow clé gérée est la clé par défaut dans le système.

2. Sélectionnez la clé active dans la table.
   La table Définition de clé s'affiche avec des informations générales sur la clé que vous ServiceNow avez générée.
3. Sélectionnez le bouton **Faire pivoter la clé** .
   Une notification s'affiche avec la possibilité de continuer la rotation de clés ou d'annuler l'opération.
4. Sélectionnez **OK** pour faire pivoter la clé.
   Un message de confirmation s'affiche en haut de la page Définition de clé.
5. Revenez à l'écran Opérations de gestion des clés pour actualiser la table Métadonnées des Chiffrement dans le cloud clés.
   Les entrées sont répertoriées pour la clé active actuelle et la clé en cours de génération pour tourner à la place de la clé active actuelle. Reportez-vous Cadre de travail de gestion des clés États clés du cycle de vie aux différents états disponibles.

   La clé active est répertoriée avec une version de `clé de 0` et la clé générée a une version de `1`.
6. Ouvrez l'entrée de la clé d'origine pour afficher les transactions de gestion des clés.
   Pour plus d'informations, consultez Transactions de gestion des clés pour plus d'informations.
   La clé précédemment active, version `0`, a été mise à jour vers l'état de cycle de vie de la clé `Tourné` et la nouvelle clé, version `1` , est `Active`.

Préparer votre clé gérée par le client

Suivez ces étapes pour préparer votre clé gérée par le client à charger sur votre instance.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Pour une clé gérée par le client, vous pouvez utiliser n'importe quelle bibliothèque cryptographique ou HSM pour générer votre clé. Cette clé doit être une clé AES 256 bits et être enveloppée d'un certificat encapsulé Chiffrement dans le cloud avec un schéma de chiffrement RSAES_OAEP_SHA_256.

Remarque :

Si vous choisissez d'utiliser l'outil de chiffrement OpenSSL pour générer votre clé, la version OpenSSL doit être la version 1.1.1x ou ultérieure.

Si vous créez et encapsulez votre clé gérée par le client à l'aide Windows de , vous devez générer la clé encapsulée via des applications de prise en charge de l'interpréteur de commandes Bash telles que Git Bash.

Procédure

1. Générez une valeur aléatoire à utiliser comme clé symétrique AES-256 bits à l'aide d'OpenSSL.

   Par exemple, en utilisant openSSL, vous pouvez générer cette clé avec la commande `openssl rand 32` .

   Pour la compatibilité, votre clé symétrique doit avoir les attributs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Valeur
Type de clé	Clé symétrique basée sur un algorithme AES (Advanced Encryption Standard).
Taille de la clé	256 bits (32 octets)
Exigence d'encapsulation de clé	○ Algorithme de chiffrement RSA ○ Remplissage de chiffrement asymétrique optimal (OAEP) ○ Fonction de hachage SHA-256 (RSAES_OAEP_SHA_256) ○ Codé à l'aide de l'algorithme Base64

2. Enregistrez la clé d'un fichier.
   Par exemple, la commande `openSSL openssl rand 32 > plaintext_key.bin` génère une clé de 32 octets et l'enregistre dans un fichier nommé `plaintext_key.bin`.

   Important :
   Enregistrez ce fichier en toute sécurité pour référence ultérieure. Cette clé est enveloppée avec la clé publique pour le téléchargement.

3. Extrayez la clé publique du fichier de certificat d'encapsulation téléchargé à partir de votre instance :

   ```
   openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
   ```

   Remarque :
   Reportez-vous à pour plus d'informations sur le téléchargement du certificat d'emballage.

4. Encapsulez la clé générée avec la clé publique téléchargée avec le certificat d'encapsulation à l'aide de l'algorithme RSAES_OAEP_SHA_256 :

   ```
   cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem -pubin -pkeyopt
    rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 | openssl base64 -A -out
    wrapped_key.txt
   ```

   Un fichier spécifié dans cette commande contient une clé gérée par le client qui peut être fournie à SN pour le processus CMK.

Basculer entre les clés ServiceNow et gérées par le client

Basculez entre une clé gérée par le client ou une ServiceNow clé gérée à utiliser dans ServiceNow Chiffrement dans le cloud.

Par défaut, votre instance est configurée pour utiliser ServiceNow des clés gérées et ServiceNow la génération de clés de chiffrement est active. Toutefois, les administrateurs peuvent choisir d'utiliser des clés gérées par le client. Ils peuvent également choisir de revenir aux ServiceNow clés gérées.

Rotation d'une clé gérée par le client

Faites pivoter votre clé gérée par le client vers votre instance après avoir enveloppé votre clé gérée par le client pour Chiffrement dans le cloud.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
   La liste des **métadonnées de Clé de chiffrement dans le cloud** se charge. Toutes les clés qui ont été utilisées dans votre instance sont répertoriées.
2. Dans la liste des **métadonnées de clé de chiffrement** dans le cloud, ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez celle dont l'état de **cycle de vie** de la clé est Actif. Il n'existe qu'une seule clé active sur votre instance.
3. Dans l'enregistrement de définition de clé, sélectionnez le bouton **Faire pivoter la clé** .
4. Dans la fenêtre **Télécharger la clé gérée par le client** , effectuez les étapes répertoriées.

   a. Sélectionnez **Télécharger le certificat d'encapsulation**.
   Le `public_certificate.... Le zip` se télécharge sur votre ordinateur local et est utilisé pour envelopper votre clé gérée par le client.

   > **⚠ Avertissement :**
   > Évitez les problèmes potentiels liés au certificat en téléchargeant le certificat d'encapsulation chaque fois que vous effectuez une rotation ou que vous basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir** pour charger votre clé gérée par le client, puis localisez et sélectionnez votre clé de chiffrement enveloppée.
   Pour choisir un autre fichier, sélectionnez le fichier et sélectionnez **Supprimer**.

   c. Fermez la fenêtre Pièces jointes.

   d. Sélectionnez **OK** pour charger votre clé.
   Si la clé est au bon format, un message de confirmation apparaît, sinon un message d'erreur s'affiche. Le fichier de clé est joint à l'enregistrement de définition de clé.

   Dans la table Transactions de gestion des clés, les étapes de téléchargement du certificat et de chargement de la clé sont énumérées. Consultez la section Transactions de gestion des clés pour en savoir plus sur les étapes de demande.

5. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour votre clé gérée par le client. Cette nouvelle clé a une valeur **Origin** de **customer_supplied** et est à l'état **Actif** . Votre clé précédente est à l'état **Pivoté** .

Basculer vers une clé gérée par le client

Utilisez votre clé gérée par le client pour ServiceNow Chiffrement dans le cloud.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Pour passer à une clé gérée par le client, vous devez disposer d'une clé gérée par le client enveloppée prête à être chargée dans le cadre de ces étapes. Pour plus d'informations sur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la préparation de cette clé pour le téléchargement, reportez-vous à la section Préparer votre clé gérée par le client. Après avoir téléchargé votre clé, ce processus lancera une rotation de clés vers votre nouvelle clé.

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
2. Dans la liste des **métadonnées de clé de chiffrement** dans le cloud, ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez celle dont l'état de **cycle de vie** de la clé est Actif. Il n'existe qu'une seule clé active sur votre instance.
3. Dans la section **Liens connexes** du formulaire, sélectionnez le lien **Basculer vers la clé gérée par le client** .
4. Dans la boîte **de dialogue Basculer vers la clé gérée par le client** , sélectionnez le bouton **Télécharger la clé gérée** .
5. Dans la boîte de dialogue **Télécharger la clé gérée par le client** , procédez comme indiqué.

   a. Sélectionnez **Télécharger le certificat d'encapsulation**.

   Avertissement :
   Évitez les problèmes potentiels liés au certificat en téléchargeant le certificat d'encapsulation chaque fois que vous effectuez une rotation ou que vous basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir**, puis suivez les instructions pour sélectionner et charger votre clé à partir de votre appareil.

   c. Sélectionnez **Basculer vers la clé gérée par le client**.

   Une demande est générée par l'instance pour passer à votre clé gérée par le client. Dans le formulaire actuel, vous pouvez voir que **l'état du cycle de vie** de la clé active à l'origine a changé sur **Pivoté**.
6. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour votre clé gérée par le client. Cette nouvelle clé a une valeur **Origin** de **customer_supplied** et est à l'état **Actif** .

Résultats

Votre instance utilise maintenant votre clé gérée par le client pour ServiceNow Chiffrement dans le cloud.

Important :
Assurez-vous qu'une copie de votre clé de chiffrement est toujours disponible dans un emplacement sécurisé pour les opérations de gestion des clés. Sans cette clé, votre instance peut être rendue inaccessible.

Basculer vers une clé gérée par ServiceNow

Revenir d'une clé gérée par le client à une clé gérée pour ServiceNow Chiffrement dans le cloud.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
2. Dans la liste des **métadonnées de clé de chiffrement** dans le cloud, ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez celle dont l'état de **cycle de vie** de la clé est Actif. Il n'existe qu'une seule clé active sur votre instance.
3. Dans la section **Liens connexes** du formulaire, sélectionnez le lien **Basculer vers la clé gérée par ServiceNow** .
4. Dans la boîte **de dialogue Basculer vers la clé gérée par ServiceNow** , sélectionnez le bouton **Basculer vers la clé gérée par ServiceNow** .
   Une demande est générée par l'instance pour passer à une ServiceNow clé gérée. Dans le formulaire actuel, vous pouvez voir que **l'état du cycle de vie** de la clé active à l'origine a changé sur **Pivoté**.
5. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour une ServiceNow clé gérée est. Cette nouvelle clé a une valeur **d'origineServiceNow** et est à l'état **Actif** .

Planifier la rotation de clés

Définissez un calendrier pour la rotation automatique de vos ServiceNow clés gérées. Ce processus met automatiquement hors service une clé de chiffrement et remplace l'ancienne clé par une nouvelle clé de chiffrement générée. Si vous utilisez une clé gérée par le client, ce calendrier peut vous rappeler de faire pivoter vos clés personnalisées manuellement.

Avant de commencer

Rôle requis : sn_kmf.admin

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Paramètres de rotations de clés planifiées**.
2. Cochez la case **Activer la rotation de clés planifiée** .
3. Renseignez les champs restants en fonction de vos besoins professionnels.

Paramètres de rotations de clés planifiées

Champ	Description
Nombre de mois entre les rotations de clés (maximum de 60 mois)	Nombre de mois entre les rotations de clés. Cette valeur est 12 par défaut et peut avoir un maximum de 60 mois.
Jour de la semaine pour effectuer la rotation de clés	Jour de la semaine où la rotation de clés est effectuée.
Heure de la journée à laquelle effectuer la rotation de clés	Heure de la journée à laquelle la rotation de clés est effectuée.
Date et heure de la prochaine rotation de clés	Date et heure de la prochaine rotation de clés planifiée. Cette valeur n'est pas modifiable directement, et est automatiquement calculée en fonction de vos choix.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre de jour avant la rotation de clés pour envoyer un rappel (maximum de 15 jours)	Nombre de jours avant la date de votre rotation de clés pendant laquelle votre instance envoie des notifications.
Les notifications par e-mail sont envoyées à la liste suivante de vos administrateurs de sécurité approuvés	Liste d'utilisateurs qui reçoivent des notifications pour la rotation de clés. **L'administrateur système** figure sur cette liste par défaut.

4. Sélectionnez **Soumettre**.
   Après avoir sélectionné Soumettre, vous pouvez voir une notification en haut du formulaire. Les notifications confirment votre rotation de clés et votre calendrier de notification.

> **⚠ Avertissement :**
>
> Chaque rotation de clés planifiée a une signature unique, qui garantit l'intégrité d'une tâche et détecte toute modification non autorisée. La signature d'une tâche planifiée est unique sur chaque instance. Clonage d'une tâche de rotation de clé planifiée d'une instance source A vers une instance cible B, la tâche planifiée sur l'instance B fera échouer la validation de signature. Si cela se produit, vous pouvez recréer la signature en décochant puis en resélectionnant la case **à cocher Activer la rotation de clés planifiée** . Pour plus de détails sur ce problème, voir KB1247113 .

Retirer une clé gérée par le client

Une fois que la fonctionnalité de retrait de clé gérée par le client est activée, une opération de retrait devient disponible dans la page Opérations de gestion des clés. Les opérations de retrait de clé et d'approbation du quorum peuvent également être gérées.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Cette section s'applique uniquement si vous disposez d'une licence Chiffrement cloud Retirer et Réapprovisionner, un module complémentaire facultatif de Chiffrement dans le cloud.

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > > **Opérations de gestion des clés**.
2. Sélectionnez la clé gérée par le client active dans la table.
   La table Définition de clé s'affiche avec des informations générales sur votre clé client. Une fonction de retrait de clé est désormais disponible.
3. Sélectionnez la **clé de retrait** pour déclencher le processus de retrait.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :

Un message d'avertissement Retirer la clé s'affiche. Le retrait de la clé déclenche un arrêt de votre instance jusqu'à ce qu'une opération de restauration soit effectuée avec la clé retirée.

DANGER :
Vous ne pouvez effectuer une opération de restauration qu'avec la même clé qui a été retirée. Si vous souhaitez passer à une autre touche, vous devez le faire après avoir restauré la clé qui a été retirée.

Si la clé gérée par le client retirée n'est pas restaurée dans le délai de ServiceNow conservation des sauvegardes (voir la SOP de sauvegarde et de restauration [procédure opérationnelle standard] pour plus de détails), les sauvegardes de la base de données de votre instance ne seront plus accessibles. Les données de sauvegarde perdues de cette manière ne sont pas récupérables.

4. Sélectionnez **OK** pour retirer la clé.
   Sélectionnez **Annuler** en cas de doute sur la fonction de retrait des clés.
   Vous revenez à l'écran Définition de clé et un message de confirmation s'affiche.
5. Actualisez la page Définition de clé pour afficher la demande de retrait en attente.



Si la politique de contrôle du quorum a été activée, le workflow d'approbation doit être terminé avec succès pour terminer le retrait de clé. Consultez Gérer le contrôle du quorum pour en savoir plus.

Fournir à nouveau une clé gérée par le client

Une fois l'opération de retrait de clé terminée, votre clé gérée par le client doit être réapprovisionnée dans votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Remarque :
Cette section s'applique uniquement si vous disposez d'une licence Chiffrement cloud Retirer et Réapprovisionner.

Procédure

1. Accéder à Now Support et accéder à **Catalogue de services** > **Catalogue** > **Gestion de l'instance** > **Restauration d'instance : réapprovisionnement des clés gérées**.
2. Cliquez sur **Demander**.
3. Dans la fenêtre **Restauration d'instance - Réapprovisionner la clé gérée** , sélectionnez votre instance dans la liste déroulante **Sélectionner une instance** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Téléchargez le certificat d'emballage en cliquant sur le texte du **certificat d'emballage** .

> **⚠ Avertissement :**
> Vous devez télécharger un nouveau certificat d'encapsulation chaque fois que vous faites pivoter ou chargez une clé gérée par le client.

5. Préparez votre clé pour le chargement.
   Pour obtenir des détails sur ce processus, consultez Préparer votre clé gérée par le client.
6. Dans la section Étape **4** , cliquez sur **Parcourir et charger** pour télécharger votre clé encapsulée à partir de votre appareil local.
   Une fois votre clé chargée, vous pouvez voir la clé sous **Téléchargé le fichier ci-dessous avec succès**.
   Si vous devez télécharger à nouveau la clé, cliquez sur **Supprimer le fichier** et chargez à nouveau votre clé comme décrit dans les étapes précédentes.
7. Cliquez sur **la touche de rotation** pour terminer le réapprovisionnement.

Politique de contrôle du quorum

La politique de contrôle du quorum spécifie le nombre minimum d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait de clé gérée par le client.

> **⚠ Avertissement :**
> Vous devez signer un addendum juridique pour activer la fonctionnalité de retrait de clé. L'option Paramètres de politique de contrôle du quorum devient disponible lorsque la fonctionnalité de retrait est activée, sinon le module n'est pas visible dans le menu de l'application. Après le retrait de la clé, votre instance n'est plus disponible tant que la clé de chiffrement n'est pas renseignée et n'est pas de nouveau active.

Dans certaines circonstances, vous voudrez peut-être créer un retrait de clé. Vous devez d'abord demander la fonctionnalité de retrait de clé auprès de Service client et assistance.

La politique de contrôle du quorum spécifie le nombre minimum d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait de clé gérée par le client. Par exemple, il y a un total de cinq approbateurs, mais seulement quatre approbations sont nécessaires pour atteindre le quorum. Lorsque quatre approbations sont obtenues, la demande de retrait est traitée et la clé retirée.

Chaque fois qu'une opération de retrait est effectuée dans un groupe activé pour l'approbation du quorum, un workflow pour l'approbation du quorum est déclenché. Une notification par e-mail est envoyée à tous les utilisateurs qui peuvent accorder l'approbation. Les tâches sont également générées dans les comptes des approbateurs, qu'ils voient sur le tableau de bord lorsqu'ils se connectent à leur ServiceNow compte.

Les utilisateurs peuvent accorder des approbations à partir de l'instance, de l'e-mail ou de la page Opérations de gestion des clés. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Une fois le nombre minimal d'approbateurs atteint, le quorum est atteint et le retrait de clé est déclenché. Le retrait est effectué et consigné, y compris les noms des utilisateurs qui ont approuvé la demande.

Consultez la section Configurer les paramètres de politique de contrôle du quorum pour plus de détails sur la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les paramètres de politique de contrôle du quorum

Suivez ces étapes pour configurer les paramètres de politique de contrôle du quorum.

Avant de commencer

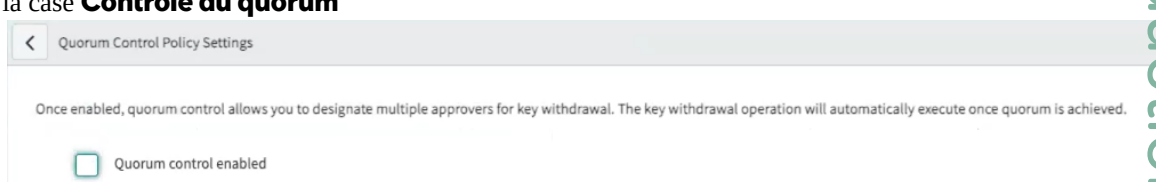
Rôles requis : sn_kmf.admin

Pourquoi et quand exécuter cette tâche

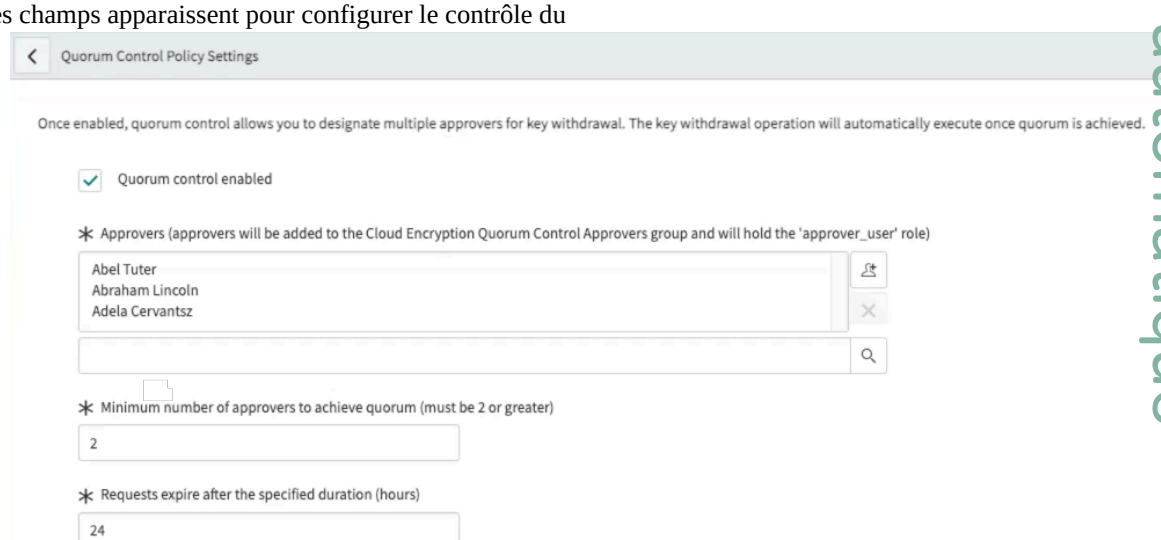
Avertissement :
Vous devez signer un addendum juridique pour activer la fonctionnalité de retrait de clé. L'option Paramètres de politique de contrôle du quorum devient disponible lorsque la fonctionnalité de retrait est activée, sinon le module n'est pas visible dans le menu de l'application. Après le retrait de la clé, votre instance n'est plus disponible tant que la clé de chiffrement n'est pas de nouveau active.

Procédure

1. Demander la fonctionnalité de retrait de clé auprès de Service client et assistance.
2. Accédez à la **Gestion de clé de chiffrement dans le cloud** > **Paramètres des politiques de contrôle du quorum**.
3. Cochez la case **Contrôle du quorum activé** .



D'autres champs apparaissent pour configurer le contrôle du quorum.



4. Renseignez les champs pour compléter le formulaire.
5. Cliquez sur **Envoyer**.
   Un message de confirmation s'affiche.

Que faire ensuite

Les actions de retrait sont disponibles dans Opérations de gestion des clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer le contrôle du quorum

Après le déclenchement d'un workflow d'opération de retrait, les actions de quorum peuvent être gérées à partir de la page Opérations de gestion des clés. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

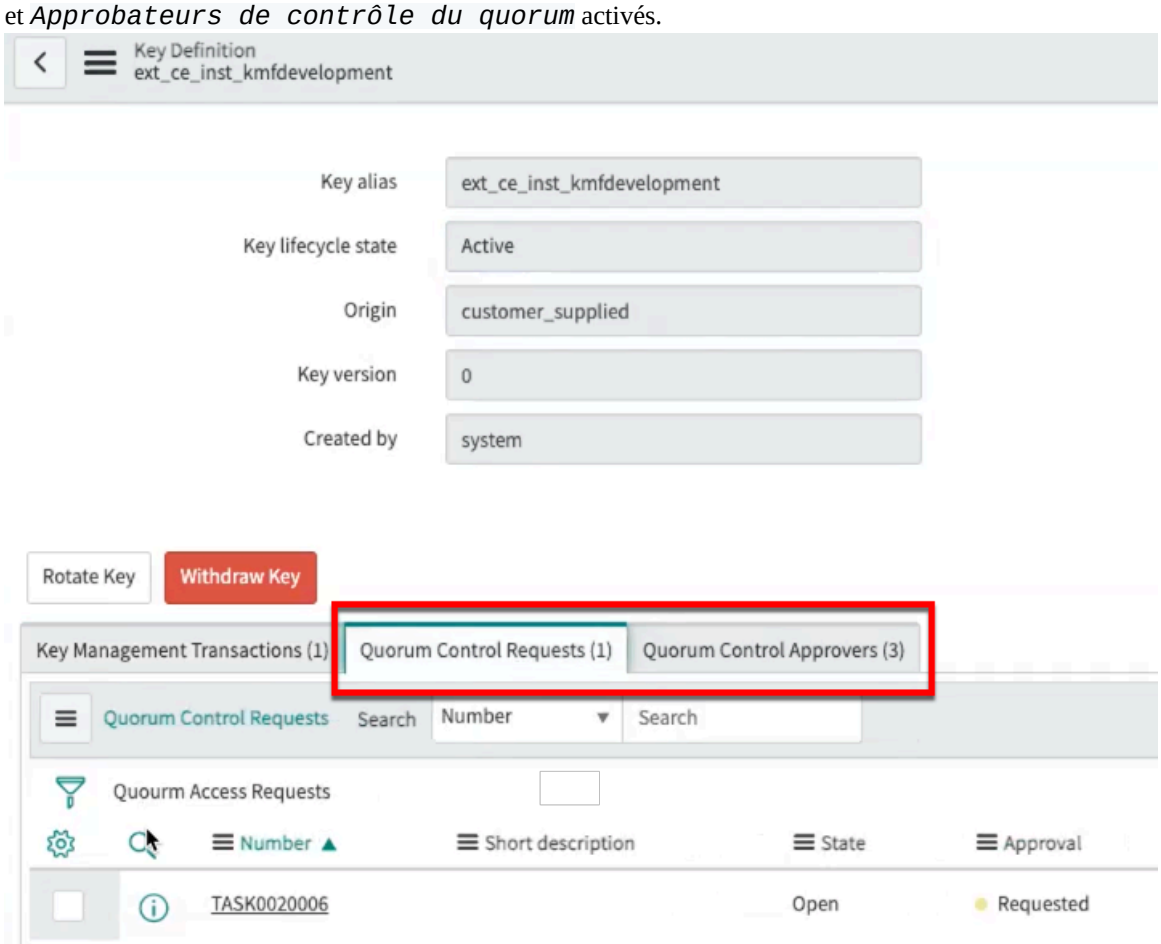
Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Lorsque le quorum a été approuvé ou rejeté, le demandeur du retrait de clé reçoit un e-mail indiquant si le quorum a été atteint ou refusé.

Procédure

1. Suivez les étapes de retrait d'une clé gérée par le client qui se trouve dans Opérations de gestion des clés.
2. Affichez les onglets *Demandes de contrôle du quorum* et *Approbateurs de contrôle du quorum* activés.



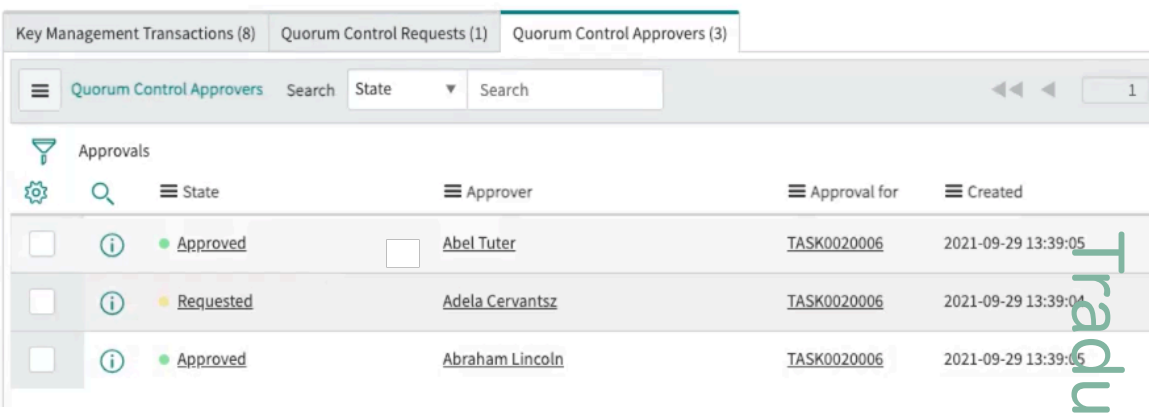
3. Ouvrez le **Demandes de contrôles du quorum** pour afficher la demande réelle créée.
   - État :
     - Ouvert : l'action de retrait de clé est en attente d'atteinte du quorum.
     - Fermé terminé : le quorum a été atteint et il ne peut y avoir aucune action complémentaire sur cette demande de quorum particulière.
   - Approbation :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Demandé : Des e-mails d'approbation ont été envoyés et le workflow a été déclenché pour atteindre le quorum.
- Approuvé : la clé sera retirée et l'instance sera arrêtée.
- Refusé : la demande de quorum est annulée et aucune autre action n'est entreprise avec cette demande. Une nouvelle demande de retrait sera nécessaire pour retirer la clé.

4. Ouvrez l'onglet Approbateurs de contrôle du quorum pour afficher la liste des approbateurs et l'état de la demande d'approbation.



État :

- Demandé : l'approbateur n'a pas encore donné suite à la demande d'approbation.
- Approuvé : la demande a été approuvée soit à partir de l'e-mail, soit à partir de la page d'approbations.

5. Sélectionnez l'onglet **Transactions de gestion des clés** pour afficher la progression de l'étape de demande de retrait de clé.
   - Étape 0 : demande de quorum : demande de quorum réelle. La demande de quorum doit être effectuée pour déclencher les étapes de retrait des clés.
   - Étape 1 - Retrait de clé : L'étape de retrait de clé. Il est composé des étapes deux à sept.
   - Étape 2 Request_preparation : crée une demande à déclencher, ainsi que l'encapsulation et la rotation.
   - Étape 3 request_integrity_check : valide que la demande est légitime et sécurisée.
   - Étape 4 request_validation : valide qu'il existe une demande en cours, une seule demande de rotation peut être traitée à la fois.
   - Étape 5 - hsm_key_delete : appelle KeySecure pour supprimer la clé active.
   - Étape 6 - key_metadata_withdraw : convertit l'état du cycle de vie des métadonnées de clé actives en « détruit ».
   - Étape 7 : post_withdraw : passe un appel pour arrêter l'instance.

Approuver ou refuser une demande de contrôle du quorum

Approuvez ou refusez une demande de contrôle du quorum à partir de Key Management Transactions.

Pourquoi et quand exécuter cette tâche

Lorsqu'une demande de quorum a été créée, le nombre minimum d'approbations est requis pour les membres. Après le déclenchement du workflow d'une opération de retrait, les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

actions de quorum peuvent être gérées à l'aide de plusieurs méthodes. Les utilisateurs peuvent accorder des approbations à partir de la page Opérations de gestion des clés, de Mes approbations dans l'instance ou directement à partir de l'e-mail de demande. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Cette procédure décrit comment approuver ou refuser une demande de quorum à partir de la page Opérations de gestion des clés.

Avant de commencer
Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Transactions de gestion des clés** > **Approbateurs de contrôle de quorum**.
2. Sélectionnez votre nom d'utilisateur dans la table.
3. Approuvez ou refusez la demande.

Approuver ou refuser une demande de quorum

Lorsqu'une demande de quorum a été créée, le nombre minimum d'approbations est requis pour les membres. Après le déclenchement du workflow d'une opération de retrait, les actions de quorum peuvent être gérées à l'aide de plusieurs méthodes. Les utilisateurs peuvent accorder des approbations à partir de la page Opérations de gestion des clés, de **Mes approbations** dans l'instance ou directement à partir de l'e-mail de demande. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Avant de commencer
Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Transactions de gestion des clés

Le sous-module Transactions de gestion des clés affiche toutes les transactions qui ont eu lieu pour les clés de votre ServiceNow instance.

- Une transaction clé est définie par les éléments suivants :
  - Composé de plusieurs étapes de demande.
  - Un seul *ID de demande* est partagé entre toutes les étapes de la demande.
  - L'étape initiale, la séquence de demande 0, d'une transaction fournit l'état actuel de la transaction globale.

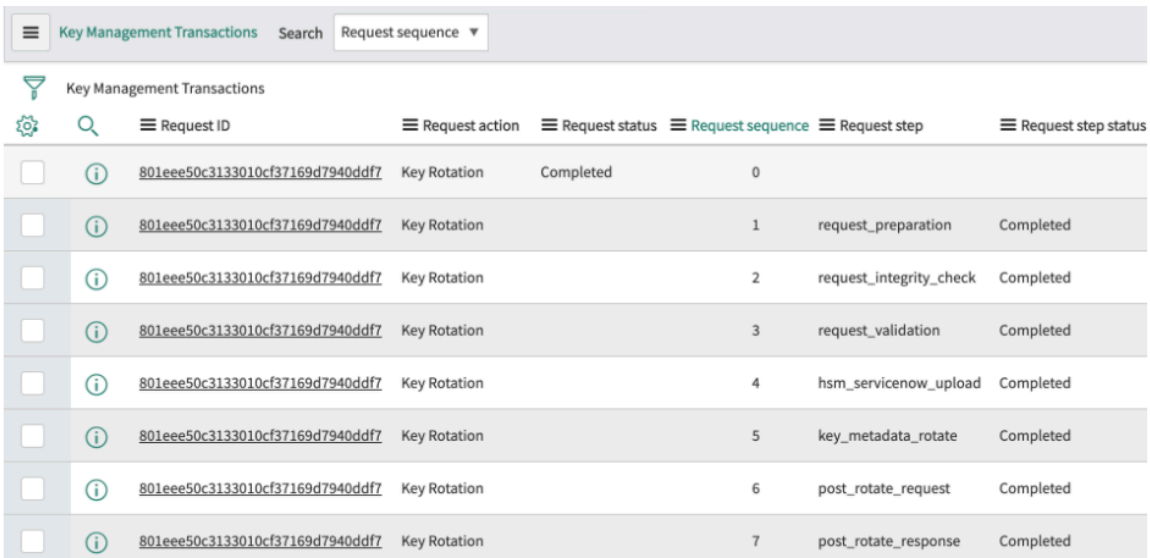
    Comme le montre l'image ci-dessous, l'étape initiale 0 a un état global de la *demande* terminé.

- Les éléments suivants peuvent être identifiés pour la transaction par l'étape de demande individuelle :
  - L'ordre de chaque étape d'une transaction peut être identifié par le numéro de séquence de l'étape.
  - L'état de chaque transaction est visible via l'état de l'étape de demande.
  - Si des étapes au-delà de l'étape initiale échouent, la transaction globale affiche l'état Échec. Si toutes les étapes sont terminées, l'état de la transaction l'est également.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’écran suivant est un échantillon du type d’informations qui s’affichent avec une ServiceNow rotation de touche.



La table suivante affiche les informations de champ disponibles sur la page Transactions de gestion des clés.

Transactions de gestion des clés

Champ	Description
ID de demande	ID unique généré par le système pour l’action en cours d’exécution Un ID de demande est partagé entre toutes les étapes de la demande.
Action de demande	Affiche l’action de l’opération clé en cours d’exécution.
Statut de la demande	• Traitement : une demande a été saisie mais n’a pas encore été terminée. • Terminé : la demande a été effectuée avec succès. • Échec : un problème s’est produit et le processus n’a pas été terminé. **Remarque :** Contactez Service client et assistance et fournissez le numéro de demande où l’échec s’est produit.
Alias de la clé	Entrée alphanumérique.
État du cycle de vie de la clé	Consultez les Cadre de travail de gestion des clés États clés du cycle de vie définitions.
Origine	• ServiceNow clé • Clé gérée par le client
Version de la clé	Lorsqu’une clé tourne, le numéro de version s’incrémente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Transactions de gestion des clés (suite)

Champ	Description
Séquence de demande	Affiche l'ordre dans lequel une demande est en cours de traitement dans le système.
Étape de demande	Affiche si une étape est en cours de traitement dans le système pendant la rotation des clés. La quantité et le contenu des étapes varient en fonction du type d'opération de clé effectuée. **1.** request_preparation : crée une demande de déclenchement, ainsi que l'encapsulation et la rotation. **2.** request_integrity_check : valide que la demande est légitime et sécurisée. **3.** request_validation : valide qu'il y a une demande en cours, qu'une seule demande de rotation peut être traitée à la fois. **4.** attachment_process : extrait le matériel de clé encapsulé de la pièce jointe. (Étape supplémentaire lors de la rotation d'une clé gérée par le client.) **5.** hsm_<Type de clé>_upload : charge le matériel de clé encapsulée dans le HSM, KeySecure. **6.** key_metadata_rotate : génère les nouvelles métadonnées de clé. **7.** post_rotate_request : envoie une demande pour effectuer la rotation de clés. **8.** post_rotate_response : réponse pour effectuer la rotation de clés en fonction de la demande de l'instance client. **Remarque :** Indiquez l'étape de demande pour Service client et assistance analyser la progression de l'état au cas où une étape de demande ne se terminerait pas.
État de l'étape de la demande	• Terminé : la rotation est réussie. • Échec : la rotation n'a pas réussi. **Remarque :** Indiquez l'étape de demande pour Service client et assistance analyser la progression de l'état au cas où une étape de demande ne se terminerait pas.

Traduction automatique

Connexion de Chiffrement dans le cloud

En savoir plus sur les options de journalisation pour Chiffrement dans le cloud.

Tables de journalisation de Chiffrement dans le cloud

Utilisez ces tables pour trouver des informations de connexion relatives aux transactions Chiffrement dans le cloud sur votre instance.

Table	Description
Métadonnées Chiffrement dans le cloud [dare_key_metadata]	Les métadonnées de chiffrement dans le cloud capturent les métadonnées clés de gestion du cycle de vie. Dans cette table, vous trouverez des informations

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	clés sur le cycle de vie, l'état et la version. Cette table est mise à jour après chaque opération de clé.
Transactions de gestion des clés [dare_key_request]	Les transactions de gestion des clés capturent les informations sur les transactions de gestion des clés. Sur cette table, vous pouvez trouver la journalisation de chaque étape d'une transaction. La table enregistre toutes les informations d'erreur pour une transaction dans le champ **de message d'erreur** .
Audits sys[sys_audit]	La table Audits sys capture les insertions et les mises à jour de tous les enregistrements audités sur votre instance. Cette table vous permet de trouver les changements apportés aux enregistrements de votre instance, le moment où ils ont été apportés et le compte d'utilisateur à l'origine du changement.

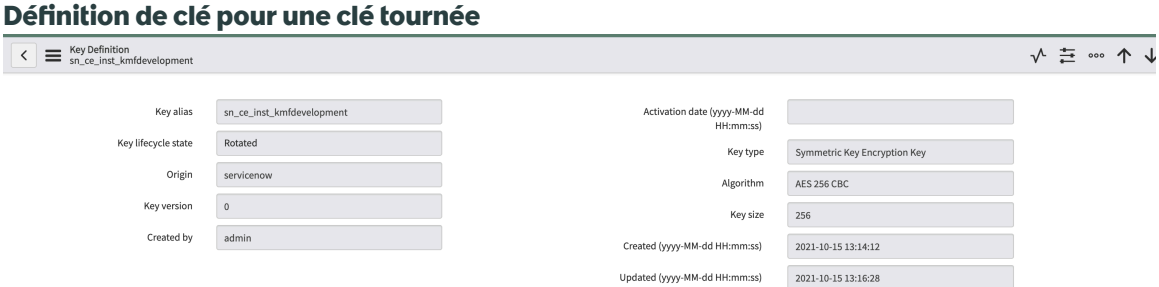
Surveiller les opérations de rotation des clés

Utilisez la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata] pour trouver des informations sur le cycle de vie de votre clé. Dans cette table, vous trouverez des informations telles que l'origine, la date d'activation, l'état et la version de vos clés.

Utilisez la table Transactions de gestion des clés [dare_key_request] pour surveiller les transactions des opérations clés. Dans cette table, vous trouverez toutes les demandes relatives à vos clés, y compris l'état, l'état et l'étape du processus dans laquelle se trouve la demande. Les demandes terminées sont conservées sur cette table avec l'état **Terminé** .

Cet exemple illustre une opération de rotation de clés. Au cours de cette opération, l'état du cycle de vie de l'ancienne clé passe d'actif à pivoté, et l'état de la version passe d'actif à retiré.

Définition de clé pour une clé tournée

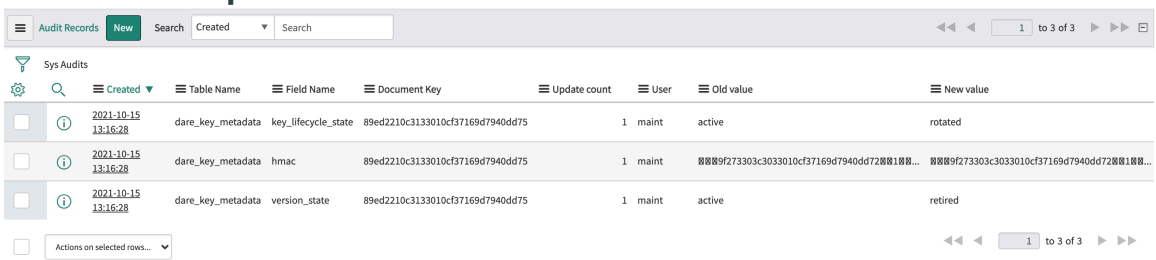


En examinant la table Audits sys[sys_audit], les administrateurs peuvent voir les changements apportés aux enregistrements dans la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata]. Les administrateurs peuvent voir quels enregistrements ont été mis à jour et quand. Les entrées de journal enregistrent également le champ qui a été modifié, ainsi que les anciennes et nouvelles valeurs.

Traduction automatique

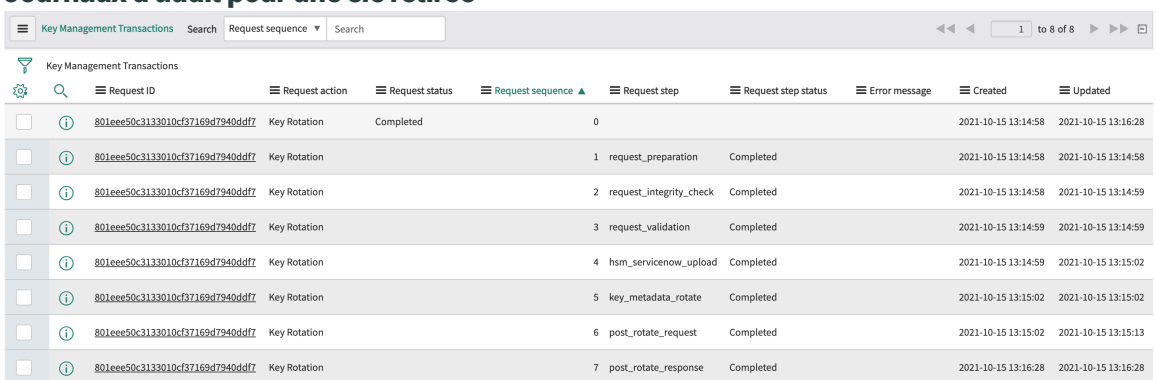
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux d'audit pour une clé retirée



Les administrateurs peuvent afficher les enregistrements dans la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata]. Dans les dossiers d'audit ci-dessous, l'état de la demande est passé de traitement à terminé.

Journaux d'audit pour une clé retirée

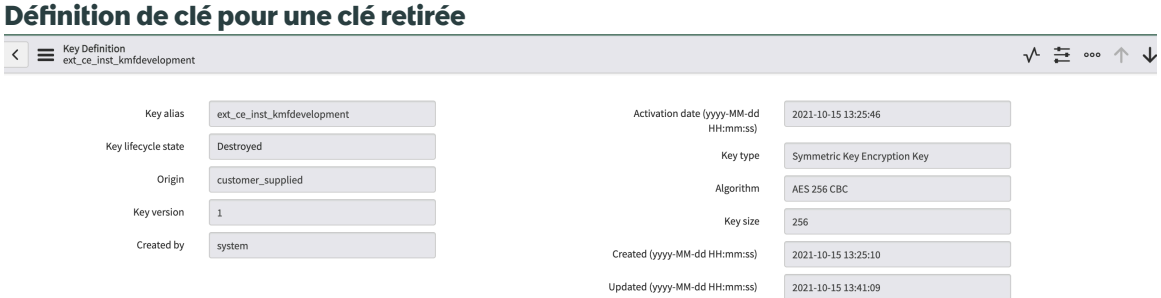


Journalisation des opérations de retrait de clés

Les informations de connexion sur le retrait des clés sont stockées dans la table Audits [sys_audit]. Ces informations de connexion contiennent des informations sur l'initiateur du retrait de clé et sur la date à laquelle le retrait a eu lieu.

Cet exemple illustre une opération de retrait de clé. Au cours de cette opération, l'état du cycle de vie de la clé passe de Généré à Actif ou Détruit. La version de la clé passe d'inconnue à active, puis hors service.

Définition de clé pour une clé retirée



En examinant la table Audits système[sys_audit], les administrateurs peuvent apporter des modifications à la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux d'audit pour une clé retirée

Audit Records | New | Search | Created | Search | 1 to 7 of 7

Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:41:09	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	2	system	active	destroyed
2021-10-15 13:41:09	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	2	system	[redacted]	[redacted]
2021-10-15 13:41:09	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	2	system	active	retired
2021-10-15 13:25:46	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	1	maint	unknown	active
2021-10-15 13:25:46	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	1	maint	generated	active
2021-10-15 13:25:46	dare_key_metadata	activation_date	7960bad0c3133010cf37169d7940dd06	1	maint		2021-10-15 20:25:46
2021-10-15 13:25:46	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	1	maint	[redacted]	[redacted]

Actions on selected rows... | 1 to 7 of 7

Détection d'altération

Utilisez la détection d'altération pour améliorer la sécurité en détectant les changements non autorisés apportés à vos paramètres de contrôle du quorum.

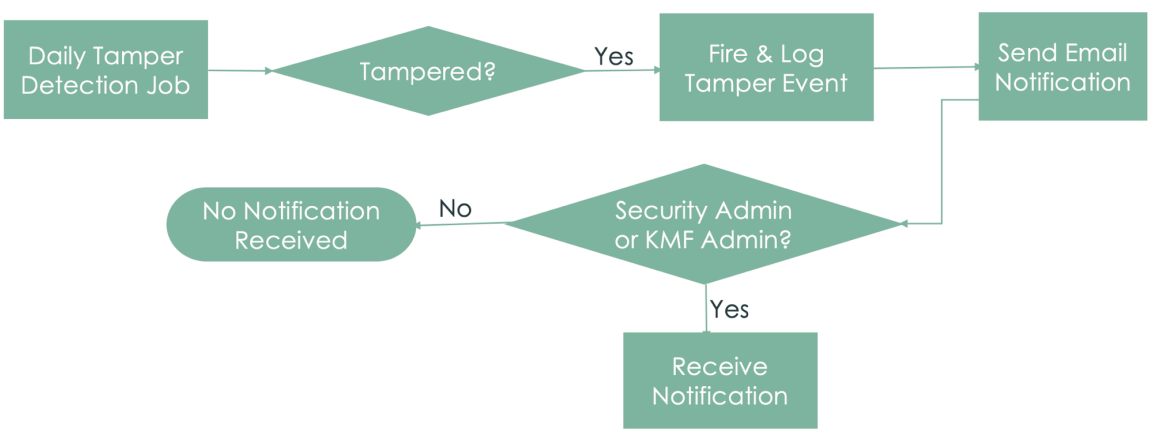
Processus de détection d'altération

Lorsqu'elle est activée, la détection d'altération valide vos paramètres de contrôle du quorum en vérifiant toute modification non autorisée (altération). La détection d'altération utilise le code d'authentification de message basé sur le hachage (HMAC).

1. Lorsqu'un paramètre est modifié ou créé, votre instance crée un HMAC. Le HMAC est basé sur la valeur de l'enregistrement de paramètre (dare_property).
2. Chaque fois que votre instance utilise ces paramètres, la détection d'altération le valide à l'aide du HMAC.
3. Si le paramètre est validé avec succès, il peut être utilisé par la plateforme, sinon ce n'est pas le cas.

La détection d'altération s'exécute quotidiennement sur votre instance

La détection d'altération vérifie la présence de falsification de vos paramètres à l'aide d'une tâche planifiée quotidienne et signale les échecs de validation dans vos journaux de nœud et de sécurité. Détection d'altération : envoyez une notification aux administrateurs de sécurité et KMF en cas d'échec de validation.

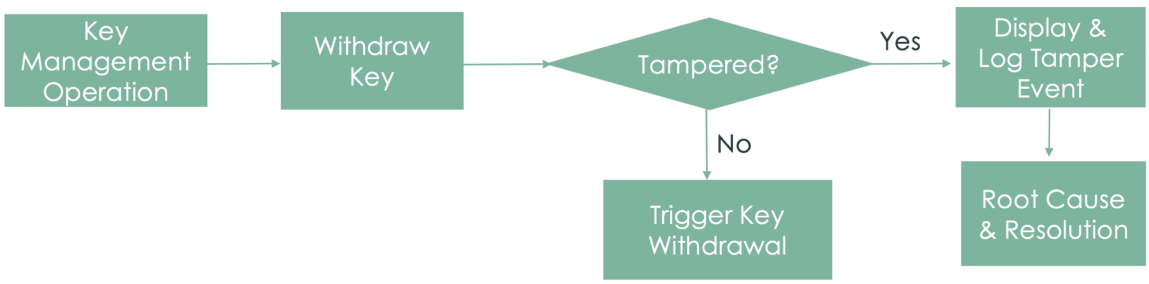


La détection d'altération s'exécute avant d'exécuter un retrait de clé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La détection d'altération valide également vos propriétés lorsque vous demandez un retrait de clé. Si vos paramètres ne passent pas la validation, le retrait de clé ne s'exécute pas. Dans ce cas, vous devez résoudre tous les problèmes de validation avant que le retrait de clé puisse concourir.



Altération de l'identification

La détection d'altération met à jour vos journaux en cas d'échec de validation.

Si la détection d'altération ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, ces échecs s'affichent dans vos journaux de nœud et de sécurité. L'entrée de journal inclut le sys_id de l'enregistrement des paramètres (dare_property) dont la validation a échoué.

```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

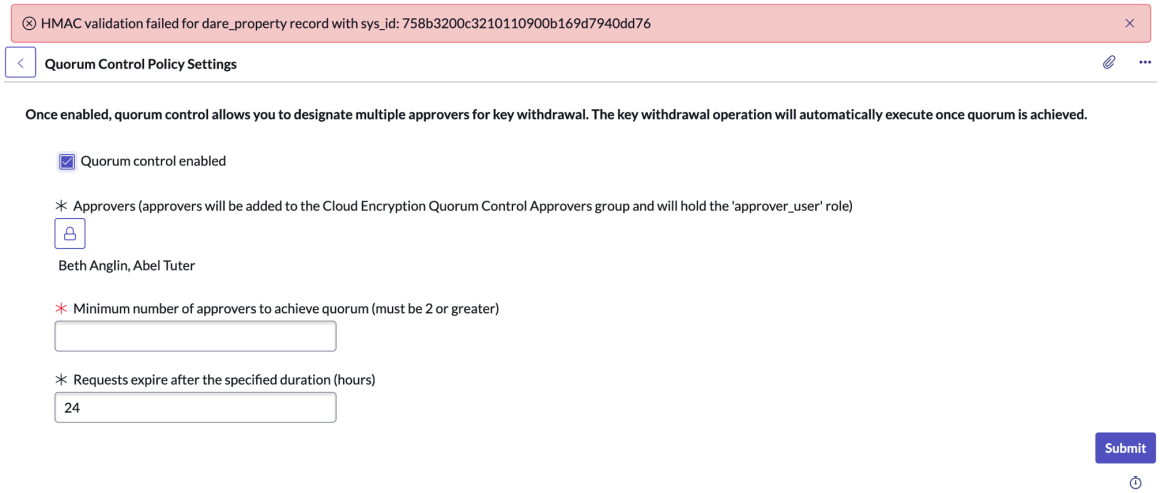
La journalisation affiche des informations similaires à ces exemples en cas d'échec de validation. Les validations réussies n'apparaissent pas dans les journaux.

Détection d'altération affiche un message d'avertissement sur votre page des paramètres de contrôle du quorum

Si la validation d'un paramètre de contrôle du quorum a échoué, un avertissement s'affiche lorsque vous consultez la page des paramètres de la politique de contrôle du quorum sur votre instance. L'avertissement inclut le sys_id de l'enregistrement des paramètres (dare_property) dont la validation a échoué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La détection d'altération envoie des notifications aux utilisateurs ayant les `Security Admin` rôles et `KMF Admin`

Si la détection d'altération ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, vos administrateurs de sécurité et vos administrateurs KMF reçoivent une notification similaire à cet exemple.

Subject: IMPORTANT: Cloud Encryption Properties Tampering Detected

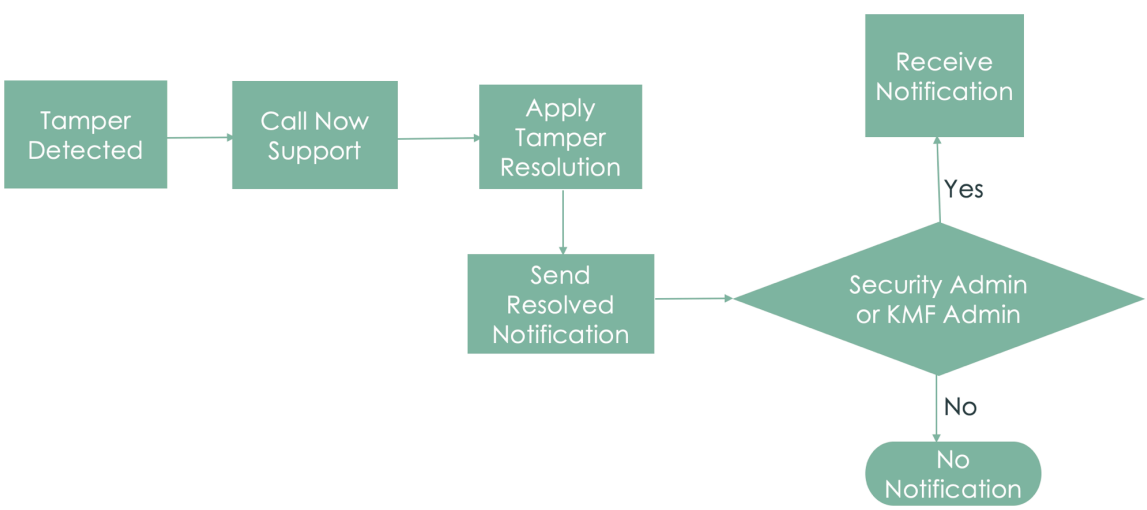
The following list of Cloud Encryption properties appear to have been tampered.
Contact ServiceNow support for additional information and how to correct this issue.

Tampered properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000109_q5pzYMS7hcgHXAoUhipc

Résolution des problèmes d'altération avec ServiceNow support

Important :
Les échecs de validation de détection d'altération ne peuvent être résolus qu'avec l'aide de l'assistance ServiceNow .

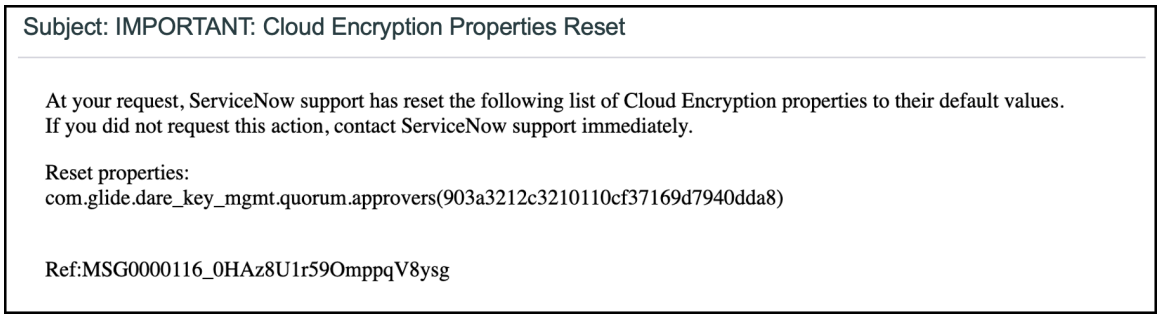


Si la détection d'altération ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, contactez ServiceNow l'assistance pour obtenir de l'aide afin de résoudre le problème. Une fois qu'un agent d'assistance a résolu l'échec de validation, les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

administrateurs de sécurité et KMF reçoivent une notification indiquant que le problème a été résolu.


Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Chiffrement intégral du disque

Le chiffrement complet du disque (FDE) applique le chiffrement à l'ensemble du système de stockage dans le serveur de base de données uniquement, car il s'agit du seul composant de stockage de données client. FDE protège uniquement contre la perte physique ou le vol des périphériques de stockage. Lorsque les serveurs de disque chiffrés sont mis sous tension et fournissent des données, le chiffrement n'offre aucune protection supplémentaire.

Chiffrement intégral du disque

Le chiffrement intégral du disque peut être pertinent pour les organisations fortement réglementées, mais peut ajouter des coûts importants au déploiement d'un ServiceNow client. Les mesures mises en place pour ServiceNow atténuer la perte ou le vol de dispositifs de stockage peuvent également être un facteur dans son choix.

Du point de ServiceNow AI Platform vue, toutes les données sont déchiffrées.

Les environnements commerciaux utilisent le chiffrement intégral du disque (FDE) avec du matériel validé FIPS 140 ou des périphériques de stockage en cours de validation, ainsi qu'une option matérielle dédiée moyennant des ServiceNow frais supplémentaires. FDE s'applique au matériel lui-même et fournit donc un cryptage au repos pour toutes les données stockées dans chaque instance qui vous est affectée.

Pour plus de détails sur la sélection des options de matériel FDE et dédié, contactez votre ServiceNow représentant.

Chiffrement Edge

ServiceNow® Chiffrement Edge ™ chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer par Internet à votre ServiceNow instance (chiffrées en vol), où elles restent chiffrées au repos.

Important :

Edge Encryption a été placé en état de fin de vente en novembre 2024 et est en phase de fin de renouvellement à partir de la version Yokohama.

ServiceNow Platform Encryption est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Fin de renouvellement de Chiffrement Edge .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



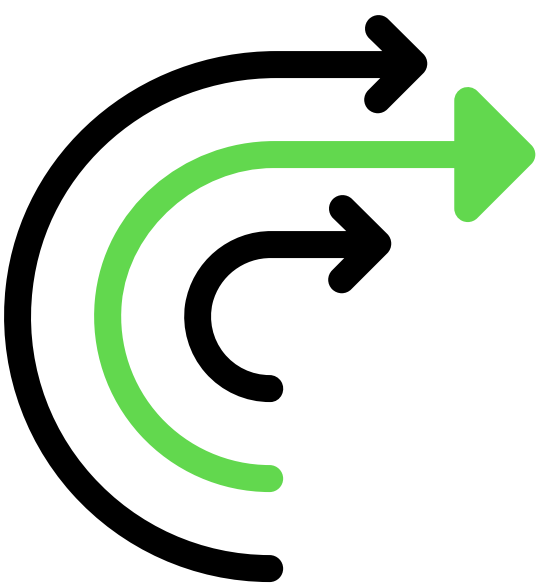
Découvrez les fonctionnalités et la valeur commerciale de Chiffrement Edge.

Plan



Découvrez comment planifier Chiffrement Edge.

Installer



Installez Chiffrement Edge.

Mise à niveau de Chiffrement Edge

Référence de mise à niveau



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Savoir comment mettre à niveau Chiffrement Edge.

Configurer



Découvrez comment configurer Chiffrement Edge.

Traduction automatique

Explorer Chiffrement Edge

Chiffrement Edge est un système de chiffrement de réseau qui réside sur votre réseau et qui chiffre et déchiffre les données sensibles lorsqu'elles transitent entre votre centre de données et le ServiceNow cloud.

Qu'est-ce que Chiffrement Edge ?

Également appelé chiffrement « côté client », Edge exige que tout le trafic bidirectionnel des utilisateurs passe par des proxys conservés sur votre infrastructure. Vous avez le contrôle total de votre gestion des clés car les clés sont stockées dans votre proxy sur votre infrastructure. Ils ServiceNow AI Platform ne peuvent pas déchiffrer votre texte chiffré pour accéder à vos clés.

Cette Chiffrement Edge fonctionnalité est une option de coût supplémentaire qui vous permet de contrôler le chiffrement de bout en bout de vos données et la gestion des clés. Chiffrement Edge utilise une application proxy, fournie par ServiceNow et installée par vous au sein de votre propre réseau. Cette application proxy segmente les schémas de données spécifiés ou chiffre les champs de chaîne, les champs de date, les champs de date/heure et les données de pièce jointe avant qu'elles ne soient envoyées de votre environnement à votre instance. L'application proxy décrypte également les mêmes données, encore une fois uniquement au sein de votre propre réseau, à l'aide de clés stockées uniquement dans votre propre réseau.

Les clés de chiffrement et la configuration pertinentes n'existent que sur le proxy Edge au sein de votre réseau et ne sont pas visibles par ServiceNow. Les données sont cryptées à

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

partir du moment où elles quittent votre environnement et ne sont décryptées qu'une fois récupérées. À aucun moment, les données ne sont accessibles en texte clair par ServiceNow les systèmes ou le personnel.

Qui utilise Chiffrement Edge

Seul un utilisateur connecté à l'instance via un serveur proxy sur votre réseau peut afficher les données chiffrées en texte clair. De même, seul un utilisateur security_admin connecté à une instance via un serveur proxy de votre réseau peut configurer et administrer Chiffrement Edge.

Étant donné que le serveur proxy réside dans votre réseau, vous possédez et gérez les clés de chiffrement, et elles ne sont jamais envoyées à l'instance. Par conséquent, n'affiche ServiceNow jamais les données sensibles en texte clair.

En plus de la configuration du proxy Edge et de la gestion des règles, vous êtes responsable des exigences habituelles liées à l'exploitation d'un serveur au sein de votre environnement (y compris l'hébergement, le routage, la sauvegarde, la configuration DNS, etc.) pour activer et prendre en charge vos proxys Edge.

Chiffrement et création de jetons

Chiffrement Edge prend en charge le chiffrement (via des configurations de chiffrement) et la tokenisation (via des modèles de chiffrement) comme moyen de protection de vos informations sensibles.

Configurations de chiffrement

Vous pouvez chiffrer des champs individuels à l'aide de configurations de chiffrement. Chiffrement Edge prend en charge les clés de chiffrement AES 128 bits et AES 256 bits. Chiffrement Edge prend en charge les types de chiffrement standard, préservant l'égalité et préservant l'ordre.

Outre les pièces jointes, vous pouvez chiffrer les types de champs suivants :

- Date
- E-mail
- Date/Heure
- HTML
- Adresse IP
- Journal
- Entrée de journal
- Texte de plusieurs lignes
- Texte sur ligne unique
- Chaîne
- URL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si un champ journal marqué pour chiffrement est ajouté au flux d'activité, toutes les entrées utilisateur dans le champ sont chiffrées dans le flux d'activité.

Les caractères codés sur plusieurs octets dans les types de champs pris en charge peuvent être chiffrés.

Vous pouvez également chiffrer les types de variables de catalogue de services suivants :

- Types de chaînes
  - Texte sur ligne unique
  - Texte de plusieurs lignes
  - Texte sur ligne unique large
- Date
- Date/Heure
- URL
- E-mail
- HTML
- Adresse IP

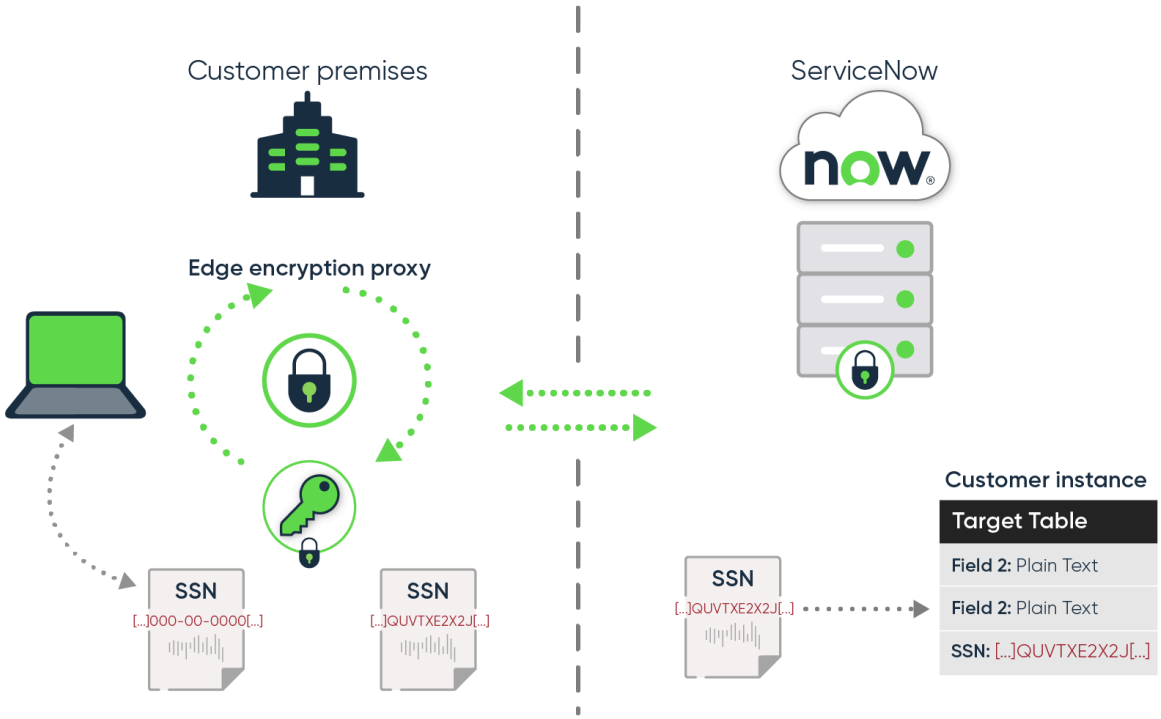
Schémas de chiffrement

Vous pouvez utiliser des modèles de chiffrement pour tokeniser des chaînes qui correspondent à des modèles réguliers, tels que les numéros de sécurité sociale et de carte de crédit. Bien que les configurations de chiffrement doivent être la principale méthode de chiffrement, utilisez des modèles de chiffrement en complément pour sécuriser les informations sensibles trouvées en dehors des champs chiffrés.

Remarque :
Le Chiffrement Edge serveur proxy nécessite une base de données MySQL dans votre réseau uniquement s'il utilise un chiffrement préservant l'ordre ou des modèles de chiffrement. Les valeurs de texte clair sont stockées dans la base de données proxy de votre réseau. Pour cette raison, il est essentiel que vous sécurisiez et sauvegardez régulièrement votre base de données proxy. Pour obtenir des recommandations, reportez-vous à la section Composants Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chiffrement Edge on the ServiceNow AI Platform

Chiffrement Edge agit comme une passerelle entre votre navigateur et votre ServiceNow instance. Le trafic provenant de votre navigateur passe par la passerelle avant d'être acheminé vers l'instance ServiceNow . La passerelle, à son tour, est configurée pour chiffrer les données sortantes marquées pour chiffrement. Le trafic entrant est déchiffré via la passerelle et l'utilisateur final voit du texte clair dans le navigateur. L'avantage de cette implémentation du point de vue du contrôle de sécurité est que le chiffrement et la gestion des clés sont gérés en externe à partir de ServiceNow.

Avantages et inconvénients

Comme pour Chiffrement de champ Enterprise et Chiffrement de champ, Chiffrement Edge impose certaines limitations fonctionnelles au sein d'une instance en raison de la sécurité supplémentaire. Cependant, le proxy Edge local fournit également des fonctionnalités supplémentaires relatives au tri par rapport au chiffrement au niveau des colonnes.

Avantages:

- Chiffrement Edge permet un contrôle absolu sur les personnes qui voient vos informations et prévient les violations de données.
- Les informations restent sur votre serveur proxy et ne quittent jamais votre réseau non crypté.
- Les informations sont chiffrées en transit, avant même d'atteindre l'instance ServiceNow .
- Vous détenez et gérez toutes vos propres clés de chiffrement. Personne d'autre, pas même ServiceNow le personnel, ne peut accéder à vos clés.
- Vous pouvez choisir la force de l'algorithme de chiffrement : AES-128 ou AES-256.
- Chiffrement Edge inclut la possibilité de chiffrer le texte de chaîne, les champs Date et Date/Heure, les pièces jointes, les URL et les journaux.
- Chiffrement Edge assure le chiffrement standard, préservation de l'égalité et préservation de l'ordre des données au repos au sein de la base de données et de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les règles de chiffrement vous permettent d'écrire des scripts personnalisés qui indiquent précisément au serveur proxy ce qu'il doit chiffrer et où placer ces informations chiffrées dans l'instance. Ces scripts sont utiles lorsque la structure de données ne correspond pas exactement à l'instance ServiceNow .
- Les modèles de chiffrement vous permettent de segmenter des informations telles que les mots de passe.

Contre:

- Chiffrement Edge nécessite un saut de réseau supplémentaire via le cluster de proxys Edge et un traitement supplémentaire, ce qui peut retarder le trafic. Le délai de traitement supplémentaire de l'application Chiffrement Edge est négligeable par rapport au saut de réseau.
- La gestion de vos propres clés de chiffrement peut être complexe et prendre du temps.
- Vous pouvez gérer un maximum de deux clés, sans possibilité de définir des clés différentes pour différents sous-ensembles de colonnes/données, ou pour différents rôles, et ainsi de suite
- Chiffrement Edge a pour effet secondaire que le serveur ou la plateforme ne peut pas déchiffrer les données pour effectuer une quelconque manipulation des données déchiffrées. Par conséquent, les ServiceNow AI Platform fonctionnalités et le traitement des données peuvent être restreints lors du chiffrement de colonnes avec Chiffrement Edge.

Ce qu'il faut savoir avant de commencer

Étant donné que le chiffrement et la tokenisation modifient la nature de vos données et peuvent Chiffrement Edge affecter d'autres processus d'instance. Avant d'utiliser Chiffrement Edge, réfléchissez attentivement à l'impact sur votre instance.

Étant donné que le serveur proxy est installé et maintenu sur votre réseau, il Chiffrement Edge nécessite une administration et une gestion réseau. Passez en revue la configuration réseau requise pour assurer une implémentation fluide.

Passez en revue les rubriques suivantes pour comprendre l'impact de Chiffrement Edge sur votre instance :

- Planification de Chiffrement Edge
- Configuration requise pour Chiffrement Edge
- Dimensionnement de votre environnement Edge Encryption
- Calculer la taille de la base de données de préservation de l'ordre et de création de jetons
- Chiffrement Edge Limitations
- Gestion des clés pour Chiffrement Edge

Composants Chiffrement Edge

Chiffrement Edge est composé du Chiffrement Edge serveur proxy qui s'exécute sur un serveur de votre réseau et du module d'extension Chiffrement Edge qui doit être installé sur votre ServiceNow instance. Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, une base de données proxy doit également être installée sur votre réseau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application proxy

Lorsque vous passez par le Chiffrement Edge serveur proxy, le module d'extension Chiffrement Edge vous permet de spécifier les champs, les modèles et les pièces jointes qui doivent être chiffrés. Vous pouvez également gérer les règles de chiffrement pour chiffrer des demandes spécifiques et planifier des tâches de chiffrement en masse.

Serveur proxy

Le Chiffrement Edge serveur proxy utilise des règles de chiffrement pour identifier dans une requête HTTP ce qui doit l'être, le cas échéant, et le chiffre avant de transmettre la demande à l'instance. Pour le déchiffrement, le Chiffrement Edge serveur proxy examine les réponses HTTP à la recherche de données chiffrées et les déchiffre avant de renvoyer la réponse au client. Pour que ce déchiffrement se produise, toutes les requêtes et réponses HTTP doivent passer par le Chiffrement Edge serveur proxy. Ces requêtes HTTP comprennent toutes les requêtes provenant d'un navigateur, ainsi que toutes les requêtes SOAP ou REST.

Base de données proxy

Si vous utilisez un chiffrement préservant l'ordre ou des modèles de chiffrement, vos serveurs proxy s'appuient sur une base de données MySQL située dans votre réseau. Tous les serveurs proxy de votre réseau doivent utiliser la même base de données.

La base de données proxy contient ces tables.

Tables de bases de données proxy

Nom	Description
db_id	ID unique de la base de données
edge_token_map	Données de modèle de chiffrement
token_map	Données de chiffrement préservant l'ordre

Sauvegarde de votre base de données proxy

Étant donné que les modèles de chiffrement reposent sur la tokenisation, les valeurs en texte clair sont stockées dans votre base de données proxy. Si la base de données est perdue, les valeurs en texte clair ne peuvent pas être restaurées. Il est essentiel que vous mainteniez des sauvegardes régulières. Pour éviter la perte de données, sauvegardez votre base de données proxy selon les ServiceNow recommandations.

- Sauvegardez votre base de données toutes les 24 heures.
- Conservez les fichiers journaux binaires de la base de données MySQL pendant au moins deux jours. Une fois qu'une sauvegarde a été restaurée, utilisez le journal binaire pour régénérer les données perdues depuis la sauvegarde la plus récente.

Chiffrement Edge Clientèle

Chiffrement Edge utilise trois clients pour informer l'instance que le proxy est en cours d'exécution, synchroniser les demandes entre le proxy et l'instance et transmettre toutes les demandes de l'utilisateur final à l'instance après tout chiffrement potentiel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Client	Description
Client Intervalle de mise à jour/KeepAlive	En charge d'envoyer une demande à l'instance ServiceNow toutes les 5 secondes pour informer l'instance que ce proxy est actif et opérationnel. Les demandes régissent le champ last_response_on sur la table du proxy Edge et, par conséquent, l'état du proxy. Si votre système rencontre des problèmes lors de l'envoi des demandes, ou si la demande ou le traitement de la demande est retardé, l'instance peut marquer le proxy comme ne répondant pas, même si les autres clients (y compris celui pour le trafic utilisateur) sont opérationnels. Ce client contrôle également l'état en ligne du proxy sur l'instance. La *edgeencryption.proxy.keepalive.interval* propriété contrôle le taux d'interrogation pour ce client. La valeur par défaut est de 5 (secondes).
Client d'interrogation/synchronisation	En charge de diverses demandes que le proxy envoie à l'instance pour qu'elle se synchronise sur la configuration de chiffrement Edge (par exemple, la table, la colonne ou la pièce jointe à chiffrer, les clés, les tâches, les règles et les modèles de création de jetons). La *edgeencryption.config.poll.interval* propriété contrôle le taux d'interrogation pour ce client. **⚠ Avertissement :** Ne modifiez pas ce paramètre. La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de synchronisation lors de la mise à jour des paramètres Chiffrement Edge sur l'instance.
Client par défaut/trafic de l'utilisateur	Pour tout le reste, ce client gère toutes les demandes des utilisateurs finaux et les transmet à l'instance ServiceNow après tout chiffrement potentiel. Ce client gère également les réponses de l'instance et les transmet à l'utilisateur final après tout déchiffrement potentiel.

Gestion des clés pour Chiffrement Edge

Vous êtes responsable de la fourniture et de la gestion des clés de chiffrement utilisées par Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette rubrique fait référence aux clés du Chiffrement Edge produit. Si vous recherchez des informations sur le cadre de gestion des clés, qui peut être utilisé avec Chiffrement de champ, voir Cadre de travail de gestion des clés.

Lors de l'obtention et de la création de clés de chiffrement prenant en charge les types de chiffrement utilisés par Chiffrement Edge, tenez compte des éléments suivants :

- Utilisation AES 128 bits ou AES 256 bits. Vous devez définir une clé de chiffrement AES 128 bits par défaut, même si elle n'est pas utilisée.
- S'il faut utiliser le système de fichiers, Java KeyStore ou la gestion des clés d'entreprise (EKM).
- Quand faire tourner les clés de chiffrement.
- Quand et si utiliser une tâche de chiffrement en masse pour chiffrer à nouveau des données à l'aide de la nouvelle clé.

Avant de supprimer une clé des fichiers de configuration du proxy et du magasin de clés, il est essentiel de déchiffrer toutes les données sur l'instance qui utilise la clé. Pour ce faire, vous pouvez ajouter une nouvelle clé de chiffrement et planifier une tâche de rotation de clés en masse.

Magasins de clés

Chiffrement Edge prend en charge les types de stockage de clés suivants.

Magasin de fichiers

Les clés sont stockées dans un fichier dans un système de fichiers accessible par le Chiffrement Edge proxy. Les clés de chiffrement stockées dans un fichier ne sont pas chiffrées, il est donc de votre responsabilité de protéger ces fichiers.

Magasin de clés Java

Les clés sont stockées dans le KeyStore JCEKS de Java. Un KeyStore Java est protégé par un mot de passe, il est donc plus sécurisé que le stockage des clés dans un fichier dans le magasin de fichiers. Un seul Java KeyStore peut stocker plusieurs clés, et les clés sont identifiées par un alias de clé, ce qui facilite la gestion de plusieurs clés.

Gestion des clés d'entreprise (EKM)

Les clés sont stockées et récupérées avec les systèmes de gestion de clés SafeNet KeySecure ou Unbound Technology.

Le Chiffrement Edge proxy est fourni avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier de magasin de clés contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow

Remarque :
Si vous utilisez un magasin de clés autre que le magasin de clés Java JCEKS du système de base, vous devez importer la ServiceNow clé publique dans votre magasin de clés. L'alias de clé publique est `servicenow`.

Outre les clés de chiffrement, le magasin de clés Java JCEKS est utilisé pour stocker la paire de clés RSA pour signer numériquement la configuration de chiffrement et les règles de chiffrement stockées dans l'instance, ainsi que le certificat numérique que le Chiffrement Edge proxy utilise pour établir une connexion sécurisée avec les navigateurs et tout autre client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des versions de clé SafeNet pour Chiffrement Edge

Utilisez la gestion des versions des clés SafeNet pour simplifier le changement de clés. Au lieu de créer un alias pour chaque nouvelle clé, la gestion des versions de clé SafeNet conserve le même alias et incrémente la version.

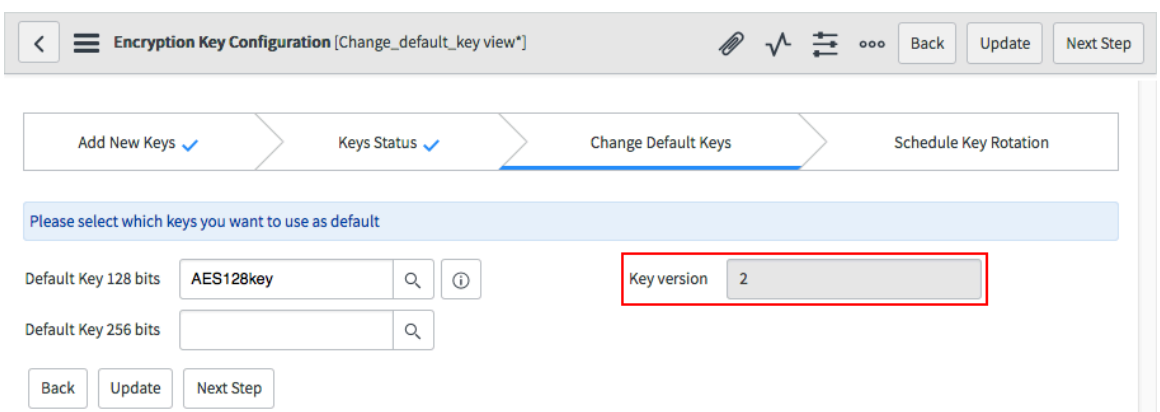
Vous devez configurer la gestion des versions des clés dans SafeNet avant de pouvoir configurer la gestion des versions des clés SafeNet sur le serveur proxy Edge.

Remarque :
Les proxys Edge installés avant la version prennent en charge les clés SafeNet, mais ne prennent pas en charge la London gestion des versions de clé SafeNet. Si vous utilisez par erreur une clé versionnée sur un proxy ou une Kingston version antérieure, lors de la mise à niveau vers une version ou une London version ultérieure, le London proxy détecte ce problème et, pour éviter une perte de données potentielle, le proxy ne démarre pas.

Vous devez d'abord planifier une tâche de rotation de clés en masse ou une tâche de rotation de clés unique pour remplacer l'ancienne clé versionnée SafeNet par une clé sans version, puis créer une nouvelle clé versionnée SafeNet, si nécessaire. Cette nouvelle clé versionnée peut être utilisée en toute sécurité avec le proxy ou une London version ultérieure, et vous pouvez redémarrer le proxy.

Configuration de la clé de chiffrement

Si vous utilisez des clés versionnées SafeNet, la section Modifier les clés par défaut du formulaire Configuration de la clé de chiffrement inclut de nouveaux champs pour la **version** de clé des clés par défaut de 128 bits et 256 bits. **Les champs de version de clé** sont grisés et ne peuvent pas être modifiés.



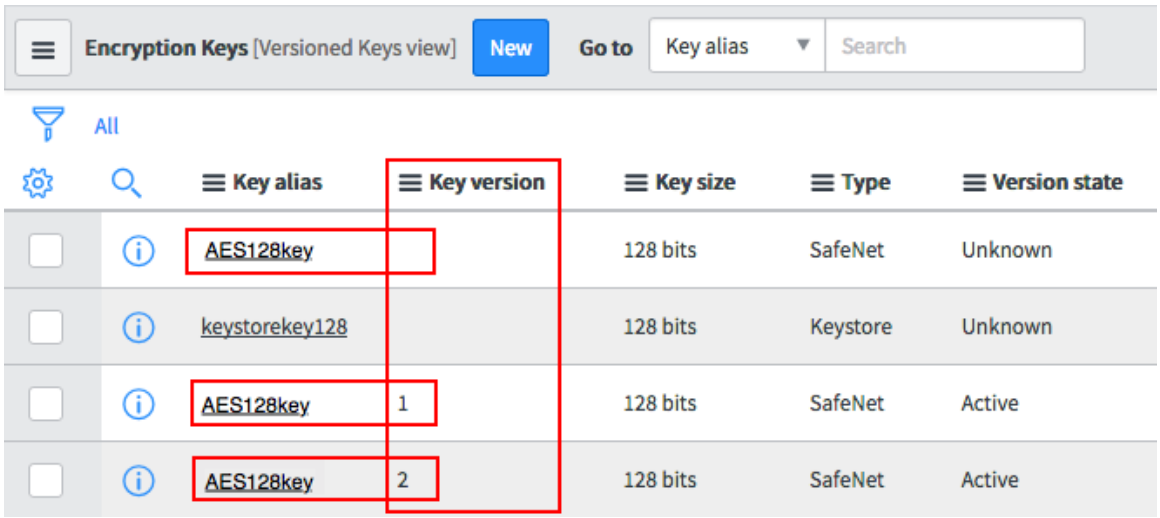
Pour les procédures, reportez-vous à la section Configurer les clés de chiffrement sur l'instance.

Clés versionnées

Si vous utilisez des clés versionnées SafeNet, lorsque vous accédez à **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Toutes les clés**, les clés versionnées incluent la version de la **clé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un numéro de version n'apparaît pas pour les entrées initiales que vous faites dans la section Modifier les clés par défaut du formulaire Configuration de la clé de chiffrement. Lorsque le serveur proxy demande une clé à SafeNet, le système ajoute une nouvelle ligne pour l'alias et ajoute la **version** de la clé.

Dans l'exemple ci-dessus, **AES128key** est répertorié trois fois :

- La première liste, sans **version de clé** indiquée, est l'entrée initiale.
- La deuxième liste, avec **1** dans la colonne **Version** de clé, est la première version de la clé renvoyée par SafeNet.
- La troisième liste, avec **2** dans la colonne **Version** de clé, est la deuxième version de la clé renvoyée par SafeNet.
- Au fur et à mesure que d'autres versions de la clé sont renvoyées par SafeNet, de nouvelles lignes sont ajoutées pour enregistrer la **version** de clé actuellement utilisée.

Configurations et schémas de chiffrement

Avec Chiffrement Edge, vous pouvez chiffrer des champs et tokeniser des chaînes.

Configurations de chiffrement

Vous pouvez chiffrer des champs individuels à l'aide de configurations de chiffrement. Chiffrement Edge prend en charge les clés de chiffrement AES 128 bits. Si les fichiers de stratégie de juridiction de force illimitée de Java Cryptography Extension (JCE) sont installés, Chiffrement Edge prend en charge les clés de chiffrement AES 256 bits pour chaque type de chiffrement. Chiffrement Edge prend en charge les types de configurations de chiffrement suivants.

Chiffrement standard

La valeur chiffrée d'un champ est différente chaque fois que le champ est chiffré, même si la valeur du champ reste la même. Le chiffrement standard est la forme de chiffrement la plus robuste. Les champs utilisant le chiffrement standard ne peuvent pas être triés, regroupés ou filtrés.

Chiffrement préservant l'égalité

La valeur chiffrée d'un champ est la même lorsque la valeur du champ reste la même. Prend en charge les comparaisons d'égalité et les opérations de regroupement par sur un champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque le chiffrement préservant l'égalité est sélectionné pour un champ qui contient déjà des données, l'exécution d'une action de regroupement sur le champ peut ne pas regrouper les champs ayant la même valeur si l'un est chiffré et l'autre non.

Cryptage préservant l'ordre

Utilise des jetons et le chiffrement pour sécuriser les données dans votre base de données proxy. Prend en charge les comparaisons d'égalité, les opérations de groupement par et la capacité de trier les données. Le type de chiffrement préservant l'ordre n'est pris en charge que si une base de données MySQL est configurée pour le Chiffrement Edge serveur proxy.

Remarque :
Lorsque vous utilisez le chiffrement préservant l'ordre et que la base de données proxy est en panne, des mises à jour peuvent être apportées aux champs à l'aide du chiffrement préservant l'ordre. Toutefois, l'ordre de tri ne sera pas correct lors de la tentative de tri des données en fonction de ces champs. Les groupes ne fonctionneront pas non plus comme prévu. Lorsque la base de données proxy est à nouveau opérationnelle, planifiez une tâche de réparation de jeton de commande pour réparer les jetons manquants.

Types de chiffrement

Les types de chiffrement suivants sont répertoriés par qualité de sécurité décroissante.

Type de chiffrement	Description
AES standard 256	Les champs ne peuvent pas être filtrés, triés ou comparés.
AES standard 128	Les champs ne peuvent pas être filtrés, triés ou comparés.
Préservation de l'égalité AES 256	Les champs peuvent être filtrés à l'aide de comparaisons d'égalité.
Préservation de l'égalité AES 128	Les champs peuvent être filtrés à l'aide de comparaisons d'égalité.
Conservation de l'ordre AES 256	Les champs peuvent être triés et le filtrage de comparaison d'égalité peut être utilisé. Nécessite l'utilisation d'une base de données MySQL dans votre réseau.
Conservation de l'ordre AES 128	Les champs peuvent être triés et le filtrage de comparaison d'égalité peut être utilisé. Nécessite l'utilisation d'une base de données MySQL dans votre réseau.

Schémas de chiffrement

Vous pouvez sécuriser les données sensibles trouvées dans les chaînes à l'aide de modèles de chiffrement. Une fois qu'un modèle de chiffrement est stocké et activé, le Chiffrement Edge serveur proxy identifie les chaînes qui correspondent au modèle dans les demandes. Une fois localisée, la chaîne de texte clair est stockée dans la base de données proxy et remplacée sur l'instance par un jeton. Utilisez des modèles de chiffrement pour créer des jetons des chaînes qui correspondent à des modèles réguliers, tels que les numéros de sécurité sociale et de carte de crédit. Bien que nous recommandions que les configurations de chiffrement soient la principale méthode de chiffrement, utilisez des modèles de chiffrement en complément pour localiser et sécuriser les informations sensibles trouvées en dehors des champs chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le Chiffrement Edge serveur proxy nécessite une base de données MySQL dans votre réseau uniquement s'il utilise un chiffrement préservant l'ordre ou des modèles de chiffrement. Les valeurs de texte clair sont stockées dans la base de données proxy de votre réseau. Pour cette raison, il est essentiel que vous sécurisiez et sauvegardez régulièrement votre base de données proxy. Pour obtenir des recommandations, reportez-vous à la section Composants Chiffrement Edge.

Information associée

Chiffrer les champs à l'aide de configurations de chiffrement

Segmenter les chaînes à l'aide de schémas de chiffrement

Composants installés avec Chiffrement Edge

Chiffrement Edge installe des tables pour stocker les données liées au chiffrement, des propriétés système pour configurer le comportement par défaut et le rôle edge_encryption à administrer Chiffrement Edge.

Tables installées avec Chiffrement Edge

Chiffrement Edge ajoute les tables suivantes.

Configuration de Chiffrement Edge [sys_encryption_configuration]

Contient des champs chiffrés et des tables pour lesquelles les pièces jointes sont chiffrées.

Règle Chiffrement Edge [sys_encryption_rule]

Contient un enregistrement pour chaque règle. Une règle a un nom, la condition lorsqu'elle est utilisée, un script et un champ d'ordre.

Journal d'insertion invalide Chiffrement Edge [sys_edge_encryption_invalid_insert_log]

Contient les messages du journal créés pour les tentatives d'enregistrement de données non chiffrées dans un champ chiffré.

Proxy Chiffrement Edge [sys_encryption_proxy]

Contient des informations sur l'application de proxy de chiffrement.

Type de chiffrement du proxy Edge [sys_proxy_encryption_type]

Utilisé pour activer et désactiver les types de chiffrement sur le formulaire de chiffrement.

Exécution de la tâche de chiffrement [sys_encryption_job_execution]

Prend en charge les tâches de chiffrement en masse.

Bloc d'exécution de la tâche de chiffrement [sys_encryption_job_execution_chunk]

Prend en charge les tâches de chiffrement en masse.

Tâche de chiffrement planifiée [sysauto_encryption_job]

Répertorie les travaux planifiés pour le chiffrement, le déchiffrement, la rotation des clés, la réparation du jeton de commande et la récupération de la base de données.

Configuration de la clé de chiffrement [sys_encryption_key_configuration]

Répertorie les clés de chiffrement par défaut.

Clé de chiffrement [sys_encryption_key]

Répertorie les clés et les attributs de clés disponibles.

Clé de chiffrement de proxy [sys_encryption_proxy_key]

Répertorie les clés de chiffrement de proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés installées avec Chiffrement Edge

Chiffrement Edge ajoute les propriétés suivantes.

Remarque :
Pour ouvrir la table Propriétés système [sys_properties], saisissez `sys_properties.list` dans le filtre de navigation.

glide.edge.pattern.disallowed.chars

Liste des caractères qui ne sont pas autorisés dans les modèles.

- **Type** : chaîne d'une liste de valeurs séparées par des virgules
- **Emplacement** : table Propriétés système [sys_properties]

glide.edge.pattern.min.size

Taille minimale du modèle autorisée. Autoriser des modèles plus petits signifie trouver plus de correspondances, ce qui augmente les frais généraux.

- **Type** : numéro
- **Valeur par défaut** : 5
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.connexion.destination

Emplacement où les messages sont consignés.

- **Type** : chaîne
- **Valeur par défaut** : fichier
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.logging.verbosité

Niveau de journalisation à utiliser.

- **Type** : chaîne
- **Valeur par défaut** : info
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

Version du proxy enregistrée auprès de votre instance.

- **Type** : chaîne
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.cleartext.allowed

Si vrai, permet d'enregistrer du texte clair dans un champ chiffré. Cela se produit lorsqu'un utilisateur accède à l'instance sans passer par le Chiffrement Edge proxy. Si la valeur est « faux », le système empêche l'enregistrement de texte clair dans un champ chiffré.

- **Type** : booléen
- **Valeur par défaut** : faux
- **Emplacement** : table Propriétés système [sys_properties]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planification de Chiffrement Edge

La mise en œuvre réussie de nécessite une planification et une Chiffrement Edge préparation.

Répondez aux questions suivantes à l'étape de la planification.

- Quels champs doivent être chiffrés ?
- Quels types de chiffrement doivent être utilisés ?
- Combien de Chiffrement Edge proxys sont nécessaires ? Consultez la section pour connaître les Dimensionnement de votre environnement Edge Encryption recommandations et les considérations.
- Si un ordre préservant le type de chiffrement ou les modèles de chiffrement doit être utilisé, où se trouve la base de données MySQL ?
- Quel système de gestion des clés doit être utilisé ?

Les administrateurs système, les administrateurs réseau et les membres de l'équipe de sécurité ont différentes tâches à accomplir pour l'implémentation Chiffrement Edge.

- Les administrateurs système ont besoin du rôle d'administrateur de sécurité. L'administrateur système doit :
  - Téléchargez l'application Chiffrement Edge proxy.
  - Configurez un Chiffrement Edge compte d'utilisateur pour que les proxys à utiliser se connectent à l'instance. Le rôle de edge_encryption doit être affecté à l'utilisateur.
  - Configurez les clés de chiffrement et définissez les clés par défaut.
  - Configurez Chiffrement Edge sur l'instance.
  - Planifiez des tâches de chiffrement.
  - Surveiller Chiffrement Edge.
  - Créez et modifiez des règles de chiffrement.
- Votre administrateur réseau doit :
  - Installez l'application Chiffrement Edge proxy.
  - Connaissez les adresses réseau des serveurs proxy et de la base de données proxy utilisée pour le chiffrement et les modèles de chiffrement préservant l'ordre.
  - Installez la base de données proxy à utiliser pour le chiffrement et les modèles de chiffrement préservant l'ordre.
  - Démarrez et arrêtez les applications proxy.
  - Effectuez la gestion de la clé de chiffrement.
  - Déterminez comment mapper les utilisateurs aux applications proxy de chiffrement. Cela peut être fait avec des paramètres DNS ou des règles de routage, et est spécifique à chaque réseau.
  - Gérez plusieurs serveurs proxy.
  - Configurez les paramètres et les pools d'équilibreurs de charge.
- Votre administrateur de sécurité doit déterminer les types de chiffrement à affecter à chaque champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration requise pour Chiffrement Edge

Vous pouvez exécuter l'application proxy sur des Chiffrement Edge serveurs ou des ordinateurs virtuels qui s'exécutent sur les systèmes d'exploitation Microsoft Windows ou Linux. Pour des performances optimales, assurez-vous que votre configuration répond à ces exigences.

Besoins Java

La machine hôte installant ou exécutant le Chiffrement Edge serveur proxy doit maintenir une version prise en charge de Java. Les versions prises en charge actuelles sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à partir de la Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant d'essayer d'installer la UtahChiffrement Edge version du proxy.

Remarque :
Java n'autorise pas automatiquement les clés de force illimitées. Vous devez spécifiquement activer l'utilisation du chiffrement AES 256 bits.

Prise en charge d'OpenJDK

Le prend en charge la version 11 d'OpenJDK ServiceNow AI Platform .

Configuration minimale du serveur proxy

Un serveur proxy nécessite cette configuration minimale :

- 4 Go de RAM par serveur proxy (6 Go sont recommandés pour la plupart des déploiements).

  Remarque :
  L'hôte du serveur proxy nécessite au moins 1 Go de RAM de plus que le serveur proxy. L'hôte du serveur proxy a besoin de 1 Go supplémentaire pour les services du système d'exploitation. Par exemple, si vous configurez un serveur proxy pour utiliser 4 Go de RAM, vous devez installer au moins 5 Go de RAM sur l'hôte du serveur proxy.

  Étant donné que le serveur proxy nécessite au moins 4 Go de mémoire, les JRE 32 bits et les systèmes d'exploitation 32 bits ne sont plus pris en charge à partir de la London version.

- Processeur 3 GHz ou plus (processeur 4 cœurs préféré pour des performances optimales).
- Plusieurs serveurs proxy derrière un équilibreur de charge. Le nombre de serveurs proxy dont vous avez besoin dépend du nombre de nœuds d'application, du nombre d'utilisateurs simultanés et du nombre de serveurs nécessaires au basculement. Consultez Dimensionnement de votre environnement Edge Encryption pour plus d'informations.
- Capacité à s'exécuter simultanément avec d'autres services, en fonction de l'utilisation du serveur et de la disponibilité des ressources.

Systèmes pris en charge par le serveur proxy

Les systèmes suivants sont pris en charge :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Système pris en charge	Description
Windows Server 2012, 2012-R2, 2016 et 2019	• Ordinateurs virtuels ou matériel physique • Systèmes 64 bits
Linux	• Ordinateurs virtuels ou matériel physique • Systèmes 64 bits Sur les systèmes Linux 64 bits, vous devez installer la bibliothèque C GNU 32 bits (glibc). La commande d'installation de CentOS est `yum install glibc.i686`.

Exigences relatives à la version du serveur proxy

Synchronisez la version de votre Chiffrement Edge proxy avec la version de votre ServiceNow instance (même version majeure, par exemple Tokyo). Pour éliminer les temps d'arrêt pendant le processus de mise à niveau, le Chiffrement Edge proxy est rétrocompatible. Cependant, il est important de mettre à niveau dès que possible pour éviter que les utilisateurs puissent accéder aux nouvelles fonctionnalités et aux corrections de bogues importantes.

Exigences de connexion au serveur proxy

Le serveur proxy qui exécute l'application doit pouvoir communiquer avec les Chiffrement Edge machines de votre réseau. Assurez-vous que le serveur proxy dispose des privilèges réseau suivants :

Privilège réseau	Description
Accès au pare-feu	Configurez les pare-feu entre le serveur proxy et les appareils clients pour autoriser une connexion. Si votre réseau utilise une zone démilitarisée (DMZ) pour ajouter une couche de sécurité supplémentaire à votre réseau local (LAN), et si vos protocoles de sécurité réseau limitent l'accès aux ports de l'intérieur du réseau vers la zone DMZ, vous devrez peut-être déployer un serveur proxy sur une machine à l'intérieur de la zone DMZ.
Accès au réseau	Configurez chaque client pour permettre au serveur proxy de s'y connecter. Si la sécurité réseau vous empêche de configurer de nouvelles machines pouvant se connecter aux clients, installez le serveur proxy sur une machine existante disposant de privilèges de connexion.
Accès à l'instance	Assurez-vous que le serveur proxy dispose d'un accès réseau à l'instance. Assurez-vous de configurer le réseau du serveur proxy pour autoriser le trafic sur le port TCP 443.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Privilège réseau	Description
Compte réseau	Installez le serveur proxy avec un administrateur local ou de domaine.

Configuration système requise pour la base de données de préservation de l'ordre et de la tokenisation

Le chiffrement et les modèles de chiffrement préservant l'ordre nécessitent la configuration d'une base de données Oracle MySQL pour le Chiffrement Edge serveur proxy. Le chiffrement préservant l'ordre permet d'appliquer directement toute opération de comparaison sur des données chiffrées, sans déchiffrer au préalable les données. Les modèles de chiffrement vous permettent de remplacer les modèles de chaîne par des jetons (appelés tokenisation) avant qu'ils ne soient envoyés et stockés dans la base de données. En raison de la taille de la base de données MySQL, utilisez un serveur proxy dédié pour exécuter la base de données de préservation de l'ordre et de tokenisation.

La configuration minimale requise pour le système de base de données est la suivante :

Base de données MySQL	Besoin
Version	Bases de données MySQL versions 5.7 et 8.0 **Remarque :** Les versions 5.5 et 5.6 de MySQL ne sont plus testées et ont atteint la fin de la prise en charge.
Systèmes d'exploitation	Systèmes 64 bits
Processeur	Processeur 2 GHz ou plus (processeur 4 cœurs préféré pour des performances optimales)
RAM	16 Go
Disque	SAN (Storage Area Network) ou stockage local (RAID 10 recommandé)
Taille	Déterminé par le nombre d'enregistrements potentiels multiplié par la taille de l'enregistrement. Voir Calculer la taille de la base de données de préservation de l'ordre et de création de jetons.
Configuration	Grappe haute disponibilité. Si vous n'êtes pas sûr de la configuration de votre serveur MySQL, contactez MySQL pour obtenir des informations de configuration.

Dimensionnement de votre environnement Edge Encryption

Le choix du nombre de serveurs proxy pour votre environnement est une tâche importante. Tenez compte du nombre d'utilisateurs, des besoins de redondance et de la latence acceptable.

Redondance

Maintenez des serveurs proxy redondants en cas de panne matérielle. Les serveurs proxy doivent être situés derrière un équilibreur de charge afin de fournir un chemin fonctionnel à tous les utilisateurs si un serveur proxy est inaccessible. Au minimum, assurez-vous que deux serveurs proxy sont toujours disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Taille

La taille fait référence au nombre de serveurs proxy requis pour éviter la latence supplémentaire produite par le chiffrement des données. Selon l'utilisation, vous pouvez réduire la latence en ajoutant des serveurs proxy supplémentaires. Par exemple, si des chiffrements de masse réguliers sont exécutés, ajoutez des serveurs proxy supplémentaires pour gérer la charge ou exécutez les chiffrements de masse lorsque la charge de l'utilisateur est légère. En outre, le matériel sur lequel le serveur proxy s'exécute influence les performances et la latence. Les serveurs proxy fonctionnant sur du matériel avec des processeurs plus rapides, plus de processeurs et plus de RAM ont un débit plus élevé que les systèmes plus lents et limités.

Les instructions suivantes supposent que votre serveur proxy fonctionne au moins sur la configuration matérielle minimale requise. Pour déterminer le nombre de serveurs proxy :

- Envisagez de configurer un serveur proxy pour deux nœuds d'application sur l'instance.
- Pour la redondance, configurez au moins deux serveurs proxy derrière un équilibreur de charge.
- Ajoutez un serveur proxy supplémentaire pour 500 utilisateurs simultanés.
- En fonction de la redondance souhaitée, ajoutez des serveurs proxy supplémentaires pour le basculement.

Par exemple, pour une instance de 2 000 utilisateurs, vous devez avoir au moins cinq serveurs proxy derrière un équilibreur de charge. Ce calcul inclut un serveur proxy pour 500 utilisateurs, avec un serveur proxy supplémentaire pour le basculement. Déterminez à l'avance quand vous approcherez d'un seuil de 500 utilisateurs et placez un autre serveur proxy dans le pool d'équilibreurs de charge.

Équilibreurs de charge

Pour équilibrer les demandes et améliorer le temps de réponse du serveur, distribuez les serveurs proxy dans un pool d'équilibreurs de charge. Configurez les équilibreurs de charge pour qu'ils utilisent la méthode « Minimum de connexions ». Cette méthode connecte les demandes au serveur proxy avec le moins de connexions actives, évitant ainsi la surcharge d'un seul proxy.

Utilisation du processeur

Le chiffrement et la tokenisation des données étant des opérations gourmandes en ressources processeur, les pics de processeur lors du chiffrement des données sont normaux et attendus. Lorsque l'utilisation du processeur est supérieure à 80 % pendant plusieurs minutes à la fois, cela signifie probablement que le serveur proxy a trop de travail à faire. Lorsque cela se produit, la latence augmente pendant la période où l'utilisation du processeur est élevée. Si la latence persiste, l'ajout d'un autre serveur proxy peut aider à réduire la latence.

Mémoire

Le serveur proxy doit disposer d'un minimum de 4 Go de RAM disponible (6 Go recommandés). Définissez les limites de mémoire initiale et supérieure du serveur proxy sur les paramètres recommandés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculer la taille de la base de données de préservation de l'ordre et de création de jetons

Si vous utilisez un chiffrement préservant l'ordre ou des modèles de chiffrement, déterminez la taille de votre base de données MySQL en multipliant le nombre d'enregistrements potentiels par la taille d'enregistrement.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Utilisez une machine dédiée pour exécuter la base de données de préservation de l'ordre et de tokenisation. N'exécutez pas la base de données sur le même matériel que le serveur proxy.

Procédure

1. Déterminez le nombre potentiel d'enregistrements qui pourraient inclure des champs chiffrés avec un chiffrement préservant l'ordre.
   a. Multipliez le nombre de configurations de chiffrement à l'aide du chiffrement préservant l'ordre par le nombre d'enregistrements auxquels chaque configuration est appliquée.
   b. Pour tenir compte de la croissance, multipliez le résultat par trois.
2. Multipliez le résultat de l'étape 1 par 1 536.
   1 536 est la taille moyenne d'un enregistrement en octets.
3. Si vous utilisez des schémas de chiffrement, effectuez les étapes 1 à 2 pour les enregistrements tokenisés et ajoutez le résultat au total.

Résultats

La valeur calculée est la taille recommandée en octets pour votre base de données de préservation de l'ordre et de tokenisation.

Chiffrement Edge Limitations

Chiffrement Edge a un impact sur les fonctions du système. Évaluez soigneusement l'impact du chiffrement d'un champ.

Restrictions de type de champ

Vous ne pouvez chiffrer que les types de champs suivants :

- Date
- E-mail
- Date/Heure
- HTML
- Adresse IP
- Journal
- Entrée de journal
- Texte de plusieurs lignes
- Texte sur ligne unique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Chaîne
- URL

Vous ne pouvez pas chiffrer les types de champs suivants :

- Champs de choix
- Champs virtuels
- Champs dans les tables système, à l'exception de certains champs dans sys_user
- Champs système dans les tables
- Champs de numérotation ou associés à un schéma de numérotation automatique
- Tout autre type de champ non répertorié ci-dessus

Restrictions supplémentaires :

- Lorsqu'un champ journal est chiffré, le bouton **Publier** est inactif, même s'il existe plusieurs champs Journal et qu'un seul de ces champs est chiffré.
- Les champs chiffrés ne sont pas disponibles dans les zones **de filtre Accéder à** et En-tête.
- Lors du chiffrement des champs utilisés comme index, vous ne pouvez utiliser que des types de chiffrement préservant l'ordre et l'égalité. Les champs indexés ne peuvent pas être chiffrés à l'aide du type de chiffrement standard.

Pour plus d'informations, voir Types de champs .

Restrictions de filtrage et de recherche

Chiffrement standard

Lorsque vous sélectionnez un champ Chaîne, Date/Heure ou URL avec une configuration de champ chiffré standard comme opérande gauche dans un filtre, aucune option de filtrage n'est disponible.

Chiffrement préservant l'égalité

Lorsque vous sélectionnez un champ Chaîne, Date, Date/Heure ou URL avec une configuration de champ chiffré préservant l'égalité comme opérande gauche dans un filtre, les opérateurs suivants sont disponibles :

- **est**
- **n'est pas**
- **est vide**
- **n'est pas vide**

Cryptage préservant l'ordre

Lorsque vous sélectionnez un champ Chaîne avec une configuration de champ chiffré préservant l'ordre comme opérande gauche dans un filtre, les opérateurs suivants sont disponibles, en plus de **est**, **n'est pas**, **est vide** et **n'est pas vide** :

- **supérieur à**
- **inférieur à**

Lorsque vous sélectionnez un champ Date ou Date/Heure avec une configuration de champ chiffré préservant l'ordre comme opérande de gauche

Traduction automatique

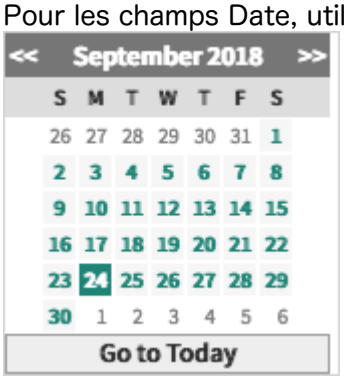
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans un filtre, les opérateurs suivants sont disponibles, en plus de **est**, **n'est pas**, **est vide** et **n'est pas vide** :

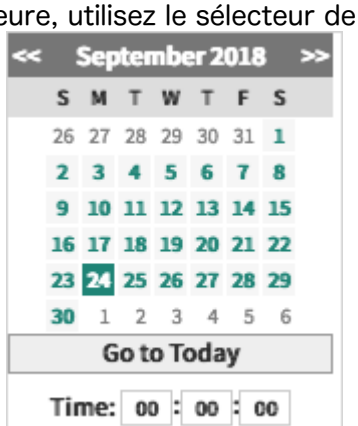
- **après**
- **avant**
- **après ou le**
- **avant ou le**

Sélecteurs de date et de date/heure

Pour les champs Date, utilisez le sélecteur de date pour spécifier la date :



Pour les champs de date/heure, utilisez le sélecteur de date et d'heure pour spécifier la date et l'heure :



Filtres de condition de liste

Les options **Afficher la correspondance** et **Filtrer** sont prises en charge dans les listes. Seules les correspondances exactes sont renvoyées ou filtrées.

Remarque :
L'ajout de champs chiffrés dans les filtres de condition est pris en charge dans les scripts tels que les politiques d'interface utilisateur et les règles métier.

Restrictions de configuration

Restrictions et comportement des configurations de chiffrement :

- Une fois que vous avez ajouté un champ à la table de Chiffrement Edge configuration, vous ne pouvez pas supprimer l'enregistrement de configuration. Si vous ne souhaitez plus chiffrer un champ, désactivez l'enregistrement dans la Chiffrement Edge table Configuration et planifiez une tâche de chiffrement pour déchiffrer les données.
- Si un champ d'une table parente est marqué comme chiffré, le champ est également chiffré dans toutes les tables héritées. Par exemple, si le champ **Brève description** de la table Tâche est chiffré, le contenu du champ **Brève description** de la table Incident est chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si un champ hérité d'une table parente est marqué comme chiffré, le champ de la table parente ne peut pas être chiffré. Par exemple, si la **description brève** de la table Incident est marquée comme étant chiffrée, la **description brève** de la table Tâche ne peut pas être chiffrée. Dans cet exemple, vous pouvez chiffrer la **description brève** dans la table Problème.
- Lorsqu'un champ avec une configuration de chiffrement définie est exporté dans n'importe quel format, la sortie inclut des valeurs chiffrées même lorsqu'elle est exportée via le serveur proxy.
- Vous ne pouvez pas importer de données dans un champ avec une configuration de chiffrement définie.
- Vous ne pouvez pas chiffrer les champs Date et Date/Heure hérités. Les champs Date ou Date/Heure hérités d'une table parente ne sont pas répertoriés dans la liste déroulante **Champ Colonne** et vous ne pouvez pas créer de configurations de chiffrement Date ou Date/Heure pour ces champs.
- Vous ne pouvez chiffrer un champ de chaîne ou d'URL qu'à partir d'une table parente ou d'une table enfant, mais pas les deux.

Restrictions d'instance

Impact de l'utilisation Chiffrement Edge sur l'instance :

- La logique back-end ne peut pas traiter les données chiffrées. Lorsque l'instance contient des données chiffrées, les règles métier, les scripts back-end ou les fonctionnalités back-end qui reposent sur l'évaluation des données dans le champ chiffré ne s'exécutent pas correctement.

> **Remarque :**
> Les données cryptées avec un cryptage préservant l'égalité ou l'ordre passent toujours les contrôles d'équivalence lorsqu'elles sont comparées à une valeur cryptée identique.

- Étant donné que le traitement des e-mails va directement des systèmes de messagerie à l'instance et ne peut pas passer par le proxy Edge, les données envoyées par e-mail ne peuvent pas être chiffrées ou déchiffrées par le proxy Edge.
  - Les données et les pièces jointes des e-mails entrants ne sont pas chiffrées.
  - Les données et les pièces jointes des e-mails sortants restent chiffrées et ne peuvent pas être déchiffrées.
- Les scripts exécutés sur le serveur ne peuvent pas modifier les données chiffrées.
- La recherche globale n'est pas prise en charge. Étant donné que la recherche globale tente de rechercher à la fois les données chiffrées et en texte clair, les résultats peuvent ne pas être ceux attendus.
- Les données chiffrées ne peuvent pas être copiées et collées dans un enregistrement où le champ n'est pas chiffré.
- Selon le type de chiffrement sélectionné, la fonctionnalité de l'interface utilisateur pour les champs chiffrés est réduite. Par exemple, la possibilité de comparer, de grouper par, de trier et de rechercher peut être affectée. En général, plus le cryptage sélectionné est fort, plus les fonctionnalités sont réduites.
- À l'exception de Java KeyStore, SafeNet et Unbound Technology, aucune gestion de clé de chiffrement logicielle ou matérielle tierce n'est prise en charge.
- Bien que plusieurs serveurs proxy connectés à une seule instance soient pris en charge, la gestion et la surveillance des clusters de proxy de chiffrement ne sont pas disponibles. Chaque proxy doit être géré séparément.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les configurations système telles que la charge de travail et le nombre de champs chiffrés peuvent avoir un impact sur les performances des champs chiffrés.
- Le Chiffrement Edge serveur proxy ne peut se connecter qu'à une seule instance.
- Si votre instance utilise une base de données Oracle et que le champ Chaîne que vous marquez pour être chiffré est supérieur à 2 925 caractères, ce champ ne peut pas être trié même lorsque le chiffrement préservant l'ordre est sélectionné.
- Si votre instance utilise une base de données Oracle, Unicode AL32UTF8 est le seul jeu de caractères pris en charge.
- Les données chiffrées ne peuvent pas être utilisées dans les rapports.
- Chiffrement Edge ne peut pas être utilisé avec l'archivage des données.
- Les proxys Chiffrement Edge ne peuvent pas chiffrer les demandes qui utilisent l'API de demande REST par lots. Si vous utilisez des proxys Chiffrement Edge, désactivez le traitement par lots REST en définissant la propriété système glide.uxf.disable_rest_batching sur true.

Installation de Chiffrement Edge

Vous pouvez installer un proxy manuellement ou à l'aide du programme d'installation Chiffrement EdgeChiffrement Edge interactif.

Besoins Java

La machine hôte installant ou exécutant le Chiffrement Edge serveur proxy doit maintenir une version prise en charge de Java. Les versions prises en charge actuelles sont Java 17.0.3 ou version ultérieure dans la série de versions 17.x.

Remarque :
Java 11 n'est plus pris en charge à partir de la version Yokohama. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 17 avant d'essayer d'installer Yokohama ou des versions ultérieures Chiffrement Edge du proxy.

Installation du serveur proxy

L'installation Chiffrement Edge comprend les étapes suivantes.

- Installez l'application Chiffrement Edge proxy sur un serveur de votre réseau à l'aide du programme d'installation interactif ou du programme d'installation manuel.
- Générez la paire de clés RSA pour signer numériquement les configurations de chiffrement et les règles de chiffrement.
- Installez Java Cryptography Extension (JCE) si vous prévoyez d'utiliser le chiffrement AES 256.
- Si vous utilisez une connexion SSL sécurisée, obtenez un certificat de serveur et importez-le dans le KeyStore Java.
- Configurez votre magasin de clés et votre clé de chiffrement.
- Si des types de chiffrement ou des modèles de chiffrement préservant l'ordre doivent être utilisés, configurez une base de données MySQL sur une machine de votre réseau.
- Définissez les propriétés souhaitées. Les propriétés se trouvent dans le fichier de configuration edgeencryption.properties .
- Spécifiez qu'un serveur proxy est une source fiable afin de Chiffrement Edge pouvoir traiter les demandes provenant de ce serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accès au serveur proxy

Une fois l'installation terminée, pointez le navigateur de chaque utilisateur vers un Chiffrement Edge proxy à l'aide du format d'URL : <host> :<port>. Les valeurs sont déterminées par les propriétés d'hôte et de port dans le fichier edgeencryption.properties .

Par exemple, avec les valeurs suivantes :

Propriété	Exemple de valeur
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Un client accède au serveur proxy à l'adresse suivante : http://hostname.mycompany.com:8081/.

Remarque :
Les paramètres DNS et les règles d'acheminement peuvent être utilisés. Les valeurs d'hôte et de port sont déterminées par votre administrateur réseau.

Demander Chiffrement Edge

Le Chiffrement Edge module d'extension (com.glide.edgeencryption) est disponible sous forme d'abonnement distinct.

Avant de commencer

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les instances de production et de sous-production de votre organisation, en général en quelques jours à peine.

Si vous n'avez pas de chargé de clientèle, si vous décidez de retarder l'activation après l'achat ou si vous souhaitez évaluer le produit sur une instance de sous-production sans frais, suivez ces étapes.

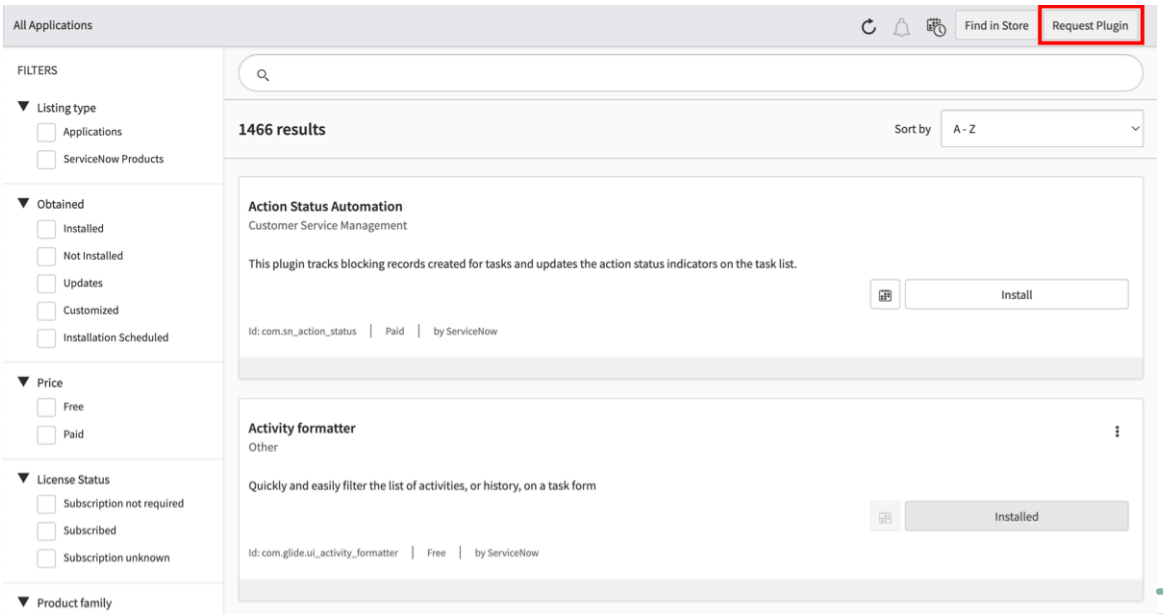
Rôle requis : aucun

Procédure

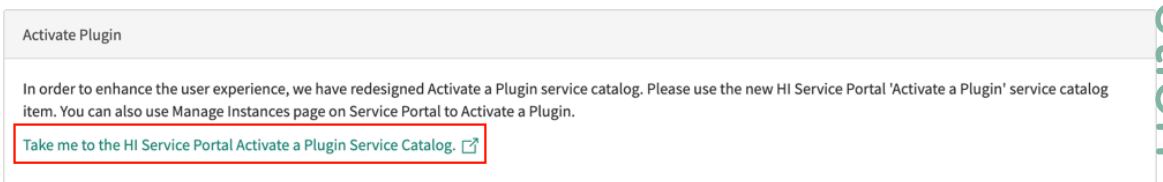
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.

Traduction automatique

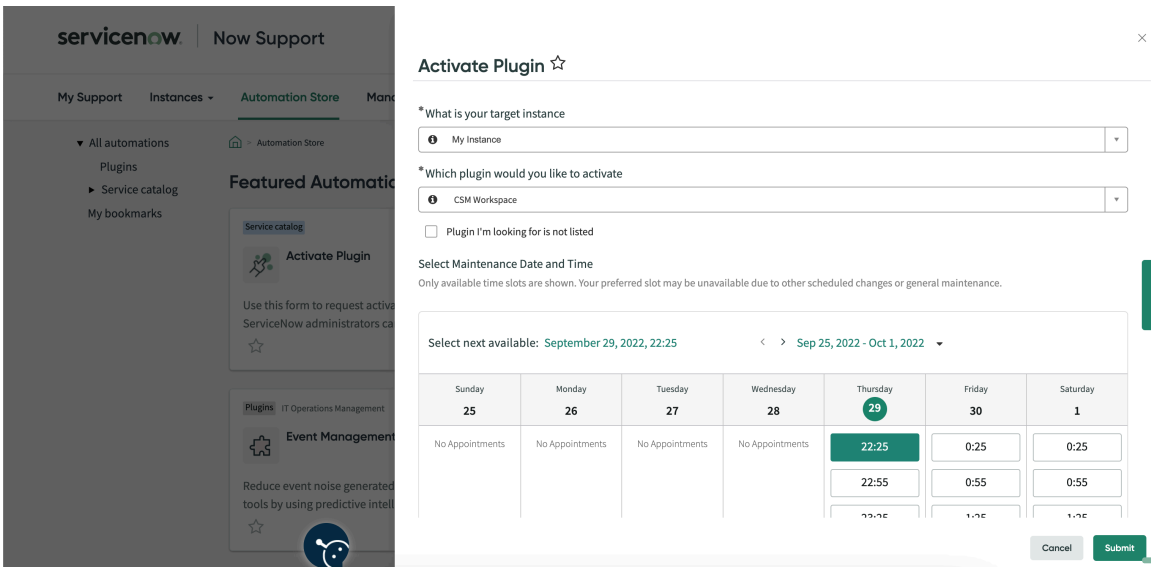
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



7. Sélectionnez **Soumettre**.
   Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Configurer un compte d'utilisateur Chiffrement Edge

Les Chiffrement Edge proxys se connectent à l'instance en tant qu'utilisateur pour obtenir et mettre à jour les informations de configuration de chiffrement. Créez un compte d'utilisateur à cet effet et donnez le rôle edge_encryption à l'utilisateur.

Avant de commencer

Le Chiffrement Edge module d'extension doit être installé avant de pouvoir affecter le rôle.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur votre ServiceNow instance, créez un compte utilisateur à utiliser par les Chiffrement Edge applications proxy.
2. Affectez le rôle de edge_encryption à l'utilisateur.

Télécharger le serveur proxy Chiffrement Edge

Téléchargez l'application Chiffrement Edge de serveur proxy à partir de votre instance, puis copiez le fichier sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Avant de commencer

Avant de commencer cette procédure, le module d'extension Chiffrement Edge doit être installé et activé sur votre instance.

Remarque :
Le Chiffrement Edge proxy est officiellement pris en charge uniquement sur Oracle JRE.

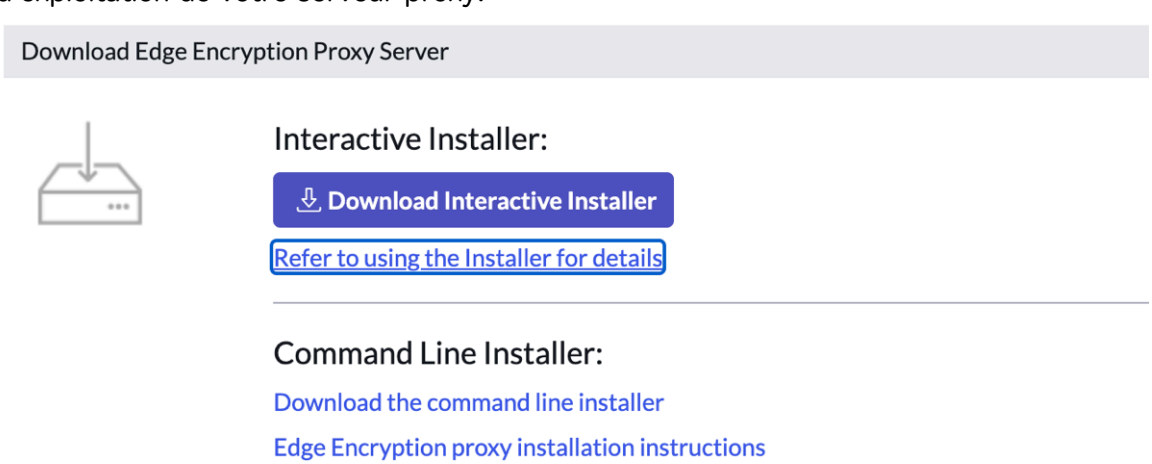
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**.
2. Pour utiliser le programme d'installation interactif, cliquez sur **Télécharger le programme d'installation interactif**.

   Si vous installez manuellement le serveur proxy, sélectionnez la version du système d'exploitation de votre serveur proxy.



Remarque :
Étant donné que le serveur proxy nécessite au moins 4 Go de mémoire pour s'exécuter, les JRE 32 bits et les systèmes d'exploitation 32 bits ne sont plus pris en charge à partir de la Washington DC version.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Copiez le programme d'installation sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Remarque :
Si vous installez manuellement le Chiffrement Edge serveur proxy, copiez le fichier ZIP sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Que faire ensuite

Après avoir téléchargé le programme d'installation Chiffrement Edge , Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation interactif. En cas d'installation manuelle, Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande.

Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation interactif

Installez le Chiffrement Edge serveur proxy sur un ordinateur Windows ou Linux à l'aide du programme d'installation interactif.

Avant de commencer

Remarque :
Les fichiers de magasin de clés SafeNet KeySecure ne sont pas pris en charge par le programme d'installation Chiffrement Edge . Pour utiliser un magasin de clés SafeNet KeySecure, Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande.

Le Chiffrement Edge module d'extension doit être installé et activé sur votre instance avant de démarrer cette procédure. Assurez-vous que la version 11.0.6 ou ultérieure de Java est installée sur l'ordinateur exécutant le programme d'installation Chiffrement Edge .

Rôle requis :

- security_admin sur votre ServiceNow instance
- administrateur local ou de domaine sur un hôte Windows
- utilisateur de service avec accès complet au système de fichiers sur un hôte Linux

Pourquoi et quand exécuter cette tâche

Après avoir installé un nouveau serveur proxy, vous pouvez exécuter à nouveau le programme d'installation pour effectuer des tests afin de détecter les problèmes d'une installation ou de modifier les paramètres actuels. Vos options incluent :

- **Installer nouveau** : installez un nouveau serveur proxy.
- **Vérifier l'installation** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente.
- **Réinstaller l'existant** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente et affichez ou modifiez les paramètres existants.

Remarque :
Si vous installez le serveur proxy sur une machine Linux sur un port privilégié (port 80 ou 443), vous devez exécuter le programme d'installation en tant qu'utilisateur racine avec un accès complet au système de fichiers. Pour restreindre l'accès au système de fichiers après l'installation du serveur proxy, vous pouvez utiliser la fonction SetUID dans le programme d'installation du proxy. Pour activer cette fonctionnalité, démarrez le programme d'installation en tant que root ou sudo root. Lorsque le programme d'installation vous y invite, indiquez le nom d'utilisateur et le groupe d'utilisateurs d'un utilisateur sans privilèges. Le serveur proxy s'installera avec les privilèges de système de fichiers de l'utilisateur donné. Vous pouvez ignorer cette étape pour continuer l'installation par défaut avec les privilèges root.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Utilisez le programme d'installation pour installer plusieurs proxys pour votre instance sur plusieurs ordinateurs, en veillant à ce que les critères suivants s'appliquent :

- Tous les proxys doivent avoir les mêmes clés de chiffrement et la même paire de clés RSA utilisées pour signer numériquement les configurations et les règles de chiffrement.
- La clé de chiffrement doit être la clé par défaut configurée sur l'instance.
- Lorsqu'une base de données proxy est configurée dans le cadre de l'installation, tous les proxys doivent utiliser la même base de données proxy.

  Vous aurez peut-être besoin d'une base de données proxy pour le chiffrement préservant l'égalité, le chiffrement préservant l'ordre ou la tokenisation. Si vous n'utilisez aucune de ces fonctionnalités, vous n'avez pas besoin d'une base de données proxy.

Que faire ensuite

Pour utiliser NVDA, un lecteur d'écran de technologie d'assistance conçu pour lire les applications Java accessibles conçues pour les utilisateurs de clavier, voir Configurer un hôte Windows 64 bits pour utiliser NVDA 32 bits avec des applications Java .

Après avoir installé le Chiffrement Edge serveur proxy, définissez la limite de mémoire initiale et la limite de mémoire de limite supérieure.

Installer le Chiffrement Edge serveur proxy (programme d'installation interactif)

Installez le Chiffrement Edge proxy sur un ordinateur Windows ou Linux.

Avant de commencer

Rôle requis : admin

Procédure

1. Téléchargez le programme d'installation du serveur proxy Chiffrement Edge.
2. Ouvrez le programme d'installation du Chiffrement Edge proxy.

   Remarque :
   Si vous effectuez l'installation sur un ordinateur Windows, vous devez exécuter le programme d'installation en tant qu'administrateur.

   a. Pour exécuter le programme d'installation en tant qu'administrateur sur un ordinateur Windows, cliquez avec le bouton droit de la souris sur l'invite de commande et sélectionnez **Exécuter en tant qu'administrateur**.

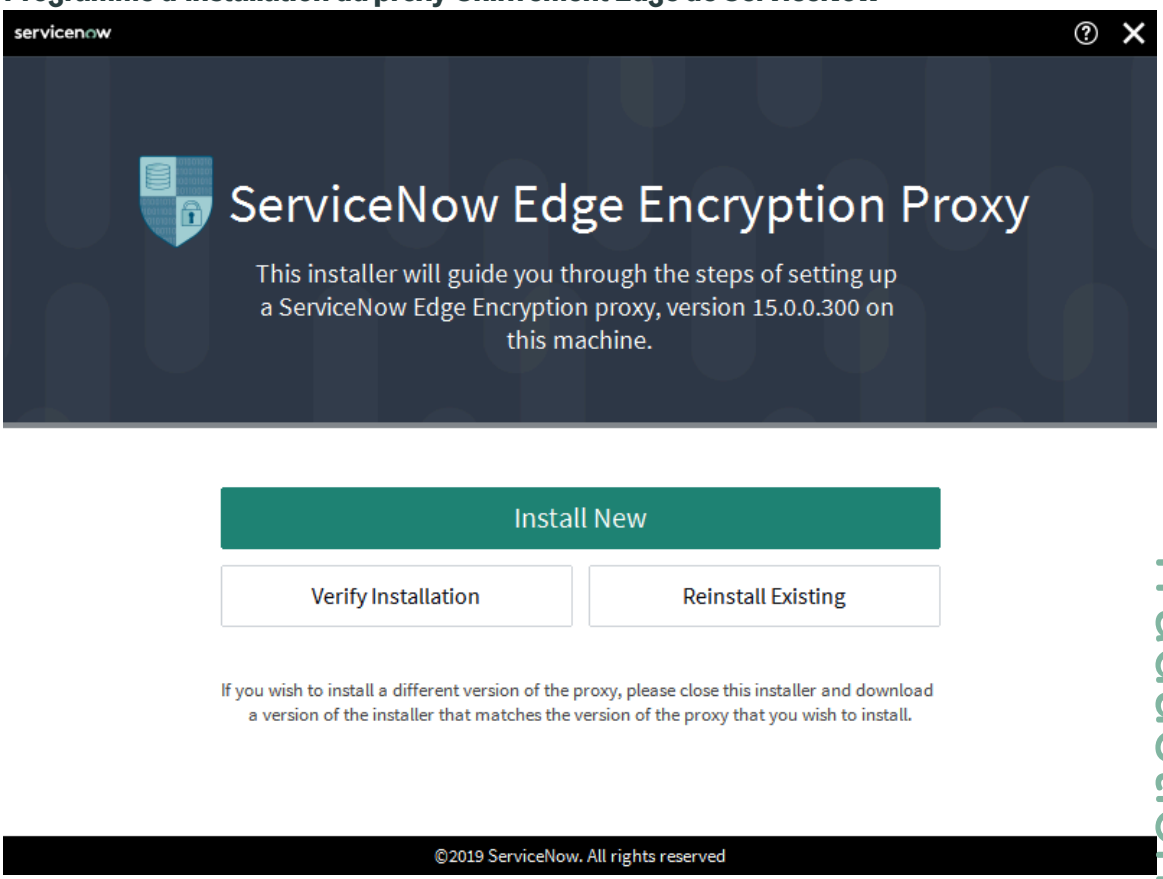
   b. À partir de la ligne de commande, accédez au répertoire qui contient le fichier .jar téléchargé.

   c. Exécutez la commande suivante : `java -jar <nom du fichier>.jar`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Programme d'installation du proxy Chiffrement Edge de ServiceNow



Traduction automatique

3. Pour installer un nouveau serveur proxy, sélectionnez **Installer nouveau**.
   Si un proxy est déjà installé, vous pouvez exécuter le programme d'installation pour :
   - **Vérifier l'installation** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente.
   - **Réinstaller l'existant** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente et affichez ou modifiez les paramètres existants.
4. Configurez **l'emplacement d'installation** et **l'instance ServiceNow cible**.

   a. Cliquez sur **Parcourir** pour sélectionner un emplacement d'installation ou saisissez manuellement un chemin d'installation.

   b. Entrez l'URL de l'instance cible ServiceNow .
   Incluez le protocole et le numéro de port.

   Example
   `https://example.servicenow.com:443`

   c. Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur disposant du rôle edge_encryption sur l'instance cible ServiceNow .

5. Cliquez sur **Suivant**.
6. Configurez les **paramètres de connexion** et les **paramètres de proxy**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Description
Hôte proxy	Nom de domaine complet de l'ordinateur sur lequel vous installez le serveur proxy. **Remarque :** Cliquez sur **Détecter le FQDN** pour rechercher le nom de domaine complet de l'ordinateur et remplir automatiquement le champ **Hôte proxy** . Avec le port, cette propriété définit l'URL utilisée par le client pour accéder au serveur proxy.
Port HTTP	Port sur le proxy pour la communication HTTP.
Port HTTPS	Port sur le proxy pour la communication HTTPS.
Nom du proxy	Nom du proxy et du service. Le nom du proxy doit être unique.
Intervalle d'interrogation du proxy	Intervalle d'interrogation en secondes. Avec le paramètre par défaut, il faut 5 secondes au proxy pour apprendre les changements de configuration de chiffrement. Les valeurs plus grandes mettent plus de temps l'instance à détecter les proxys mis en ligne. **Remarque :** La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lors de la mise en ligne d'un proxy.
Intervalle d'envoi de ping de conservation de connexion active au proxy	Durée, en secondes, entre les pings émis par le proxy à l'instance. Des pings sont émis périodiquement pour vérifier la connectivité entre le proxy et l'instance. La valeur par défaut est de 10. La valeur minimale est 5.

Traduction automatique

7. Cliquez sur **Installer**.
   Le Chiffrement Edge serveur proxy est installé. L'installation peut prendre quelques minutes.

Configurer la protection des propriétés de CyberArk

En option, configurez la protection des propriétés de CyberArk pour stocker Chiffrement Edge en toute sécurité les mots de passe dans un coffre-fort numérique centralisé et sécurisé.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous devez acheter et configurer CyberArk AIM (Application Identity Management) avant de pouvoir configurer les paramètres de connexion et les informations d'identification protégées de CyberArk pour un serveur proxy. Dans le cadre de l'installation du client AIM, le fichier JavaPasswordSDK.jar est installé

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans le répertoire d'installation du client AIM. Le coffre-fort de CyberArk est installé sur un serveur renforcé indépendant, et les clients AIM permettent un accès sécurisé à ce serveur.

Remarque :
Vous devez installer le client CyberArk AIM sur chaque ordinateur hôte sur lequel un proxy Edge est installé.

Dans le programme d'installation d'Edge, vous devez spécifier l'emplacement du fichier JavaPasswordSDK.jar pour configurer la connexion de CyberArk au proxy Edge. Vous devez également entrer d'autres valeurs que vous avez définies lors de l'installation du client AIM.

La configuration du stockage des mots de passe CyberArk est facultative. Si vous ne souhaitez pas configurer le stockage des mots de passe CyberArk, cliquez sur **Ignorer** les écrans de CyberArk.

Procédure

1. Sur la page Connexion CyberArk du programme d'installation, entrez les paramètres de Chiffrement Edge connexion CyberArk.

Paramètres de connexion de CyberArk

Paramètre	Description
Chemin d'accès à PasswordSDK.jar	Le chemin vers le fichier JavaPasswordSDK.jar installé sur l'ordinateur Windows hôte pendant la configuration de CyberArk.
ID d'application	**L'ID d'application** saisi lors de la configuration de CyberArk.
Nom sûr	Nom **du coffre-fort** saisi lors de la configuration de CyberArk.

2. Cliquez sur **Suivant**.
3. Sur la page Informations d'identification protégées de CyberArk du programme d'installation, saisissez les informations d'identification à protéger par CyberArk.
   - Pour utiliser un seul nom d'information d'identification pour tous les mots de passe protégés, cochez la case **Appliquer un nom d'information d'identification à toutes les informations d'identification** , saisissez le nom des informations d'identification et cliquez sur **Appliquer**.
   - Entrez le nom des informations d'identification pour un ou plusieurs des champs suivants. Les noms d'informations d'identification sont les noms d'utilisateur saisis pour les clés SSH lors de la configuration de CyberArk.

Informations d'identification protégées CyberArk

Paramètre	Description
Utilisateur de Chiffrement Edge	Nom des informations d'identification CyberArk d'un utilisateur de chiffrement Edge.
Magasin de clés de clé de signature	Nom des informations d'identification CyberArk pour le magasin de clés de signature.
Magasin de clés de certificat HTTPS	Nom des informations d'identification CyberArk pour le magasin de clés de certification HTTPS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Description
Magasin de clés de chiffrement	Nom des informations d'identification CyberArk du magasin de clés de chiffrement.
Base de données	Nom des informations d'identification CyberArk du magasin de clés de base de données.
Magasin de clés de certification HTTPS SafeNet	Nom des informations d'identification CyberArk du magasin de clés de certification HTTPS SafeNet.
Serveur SafeNet	Nom des informations d'identification CyberArk pour le serveur SafeNet.
Transférer le proxy	Nom des informations d'identification CyberArk pour le proxy de transfert.

4. Cliquez sur **Suivant**.

Configurer la clé de signature

Configurez la clé de signature après l'installation du serveur proxy via le programme d'installation du Chiffrement Edge proxy.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La clé de signature signe les modifications apportées aux configurations et aux propriétés par le serveur proxy. La clé de signature doit être une paire de clés RSA asymétrique dans un magasin de clés JCEKS.

Remarque :
Si vous installez plusieurs proxys, chaque proxy doit utiliser la même clé de signature.

Procédure

1. Sur la page Clé de signature du programme d'installation Chiffrement Edge , sélectionnez le magasin de clés sur l'ordinateur hôte pour stocker la clé de signature.
   - **Créer un nouveau magasin de clés Java** : entrez l'emplacement du répertoire, le nom et le mot de passe du nouveau magasin de clés.
   - **Utiliser le magasin de clés existant** : entrez l'emplacement et le mot de passe du fichier de magasin de clés.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou créez une clé de signature.
   - **Nouvelle clé** : créez une clé de signature pour ce proxy.
   - **Utiliser une clé existante** : utilisez une paire de clés RSA du magasin de clés sélectionné.
   - **Importer la clé existante** : importez une paire de clés RSA à partir d'un magasin de clés différent. Accédez au fichier du magasin de clés, entrez le mot de passe du magasin de clés et sélectionnez l'alias de clé. Fournissez un nouvel alias pour la clé.
4. Cliquez sur **Suivant**.

Configurer le certificat HTTPS

Pour permettre aux clients de se connecter au serveur proxy à l'aide Chiffrement Edge d'une connexion SSL sécurisée, importez le certificat HTTPS sur le serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Le Chiffrement Edge proxy fournit le certificat HTTPS aux clients qui tentent de se connecter.

Procédure

1. Sur la page Certificat HTTPS du programme d'installation Chiffrement Edge , sélectionnez le magasin de clés pour stocker le certificat.
   - **Créer un nouveau magasin de clés Java** : entrez l'emplacement du répertoire, le nom et le mot de passe du nouveau magasin de clés.
   - **Utiliser le magasin de clés existant** : entrez l'emplacement et le mot de passe du fichier de magasin de clés.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou importez un certificat.
   L'alias de clé est l'alias donné pour le certificat.
   - **Utiliser un certificat existant** : utilisez un certificat existant dans le magasin de clés sélectionné.
   - **Importer à partir d'un fichier ou d'un magasin de clés** : importez un certificat à partir d'un autre magasin de clés ou d'un fichier .cer. Accédez au magasin de clés ou au fichier .cer, entrez le mot de passe et sélectionnez l'alias. Vous devez fournir un nouvel alias pour le certificat.
4. Cliquez sur **Suivant**.

Configurer la clé de chiffrement AES 128 bits

Après avoir configuré le certificat HTTPS via le programme d'installation Chiffrement Edge proxy, configurez la clé de chiffrement AES 128 bits pour chiffrer vos données.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La clé de chiffrement est soit un fichier texte brut dans le répertoire `/keys` , soit une clé secrète dans un magasin de clés. Si vous utilisez un magasin de clés pour vos clés de chiffrement AES 128 bits et AES 256 bits, elles doivent utiliser le même magasin de clés.

Si vous mettez à jour un certificat SSL sur un serveur proxy Edge, consultez Mettre à jour le certificat SSL.

Procédure

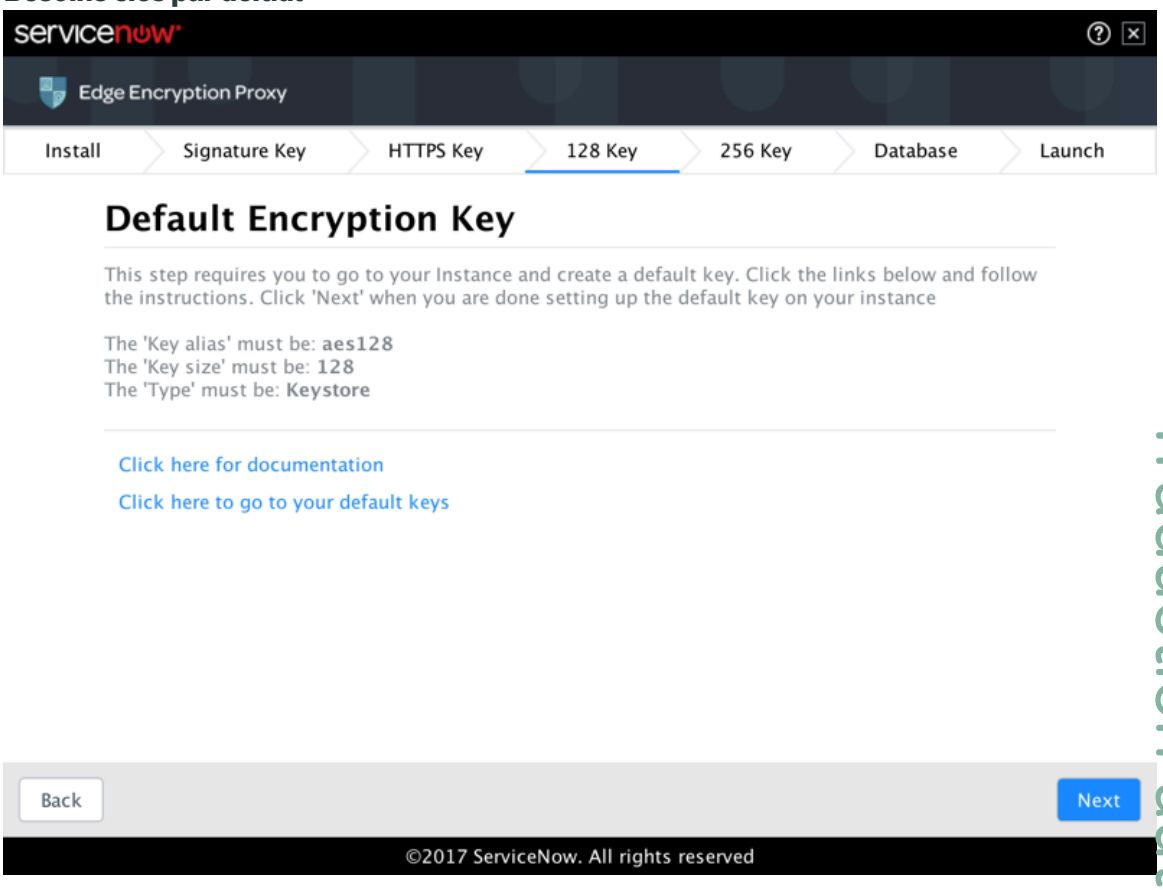
1. Sélectionnez l'emplacement de la clé de chiffrement.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou créez la clé de chiffrement.
4. Cliquez sur **Suivant**.
5. Configurez la clé sur l'instance en fonction des exigences définies dans votre programme d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour configurer la clé sur l'instance, accédez à l'instance et définissez une clé par défaut. Voir Configurer les clés de chiffrement sur l'instance. Assurez-vous que l'alias, la taille et le type de clé correspondent aux exigences définies dans le programme d'installation.

Besoins clés par défaut



6. Une fois la clé configurée sur l'instance, revenez au programme d'installation et cliquez sur **Suivant**.

Configurer la clé de chiffrement AES 256 bits

Après avoir configuré la clé AES 128 bits via le programme d'installation du proxy Edge, vous pouvez éventuellement configurer une clé de chiffrement AES 256 bits pour chiffrer vos données.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La clé de chiffrement est soit un fichier texte brut dans le répertoire /keys , soit une clé secrète dans un magasin de clés. Si vous utilisez un magasin de clés pour vos clés de chiffrement AES 128 bits et AES 256 bits, les deux clés doivent utiliser le même magasin de clés. Si vous ne souhaitez pas configurer une clé de chiffrement AES 256 bits, sélectionnez **Ignorer** pour continuer l'installation du serveur proxy.

Si vous mettez à jour un certificat SSL sur un serveur proxy Edge, consultez Mettre à jour le certificat SSL.

Procédure

1. Sélectionnez l'emplacement de la clé de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez **Suivant**.
3. Sélectionnez ou créez la clé de chiffrement.
4. Sélectionnez **Suivant**.
5. **Facultatif :** Si vous souhaitez utiliser le cryptage AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.
6. Pour utiliser le chiffrement AES 256 bits, vous devez également configurer la clé de chiffrement AES 256 bits par défaut sur l'instance.

   Pour ce faire, accédez à l'instance et définissez une clé par défaut. Consultez Configurer les clés de chiffrement sur l'instance. Assurez-vous que l'alias, la taille et le type de clé correspondent aux exigences définies dans le programme d'installation.
7. Une fois la clé configurée sur l'instance, revenez au programme d'installation et sélectionnez **Suivant**.

Mettre à jour le certificat SSL

Lors de la mise à jour d'un certificat SSL sur un serveur proxy Edge, vous devez supprimer l'ancien.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Lors de la mise à jour du certificat SSL sur le serveur proxy Edge, vous devez également supprimer l'ancien certificat. Si ce n'est pas le cas, l'ancien certificat (sous la forme d'un alias dans le fichier KeyStore) continue d'être utilisé même si le serveur proxy Edge est configuré pour utiliser le nouveau certificat.

Procédure

1. Sur le serveur proxy Edge, répertoriez les entrées dans le KeyStore Java :

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
```

2. Supprimer l'ancien certificat SSL :

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

3. Ajoutez le nouveau certificat SSL dans le KeyStore Java.

Configurer la base de données proxy Chiffrement Edge

Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, vous pouvez éventuellement configurer les propriétés de la Chiffrement Edge base de données proxy.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Pour utiliser des types de chiffrement ou des modèles de chiffrement préservant l'ordre, une base de données MySQL s'exécutant sur votre réseau est obligatoire. Cette tâche connecte le proxy à la base de données, mais elle n'installe ni ne configure la base de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
En cas d'utilisation de plusieurs serveurs proxy, tous les serveurs proxy doivent utiliser la même base de données proxy. Les valeurs saisies dans le programme d'installation doivent être les mêmes pour tous les serveurs proxy.

Procédure

1. Confirmez ou modifiez l'URL de la base de données, qui est l'emplacement de la base de données proxy.
2. Dans le champ **Nom** , entrez le nom de la base de données proxy.
   La valeur par défaut est `edgeencryption`.
3. Entrez le nom d'utilisateur et le mot de passe pour accéder à la base de données proxy.
4. Cliquez sur **Suivant**.

Lancer le serveur proxy Chiffrement Edge

Une fois qu'un Chiffrement Edge proxy est installé et configuré, vous pouvez le démarrer à partir du programme d'installation.

Avant de commencer
Rôle requis : admin

Procédure

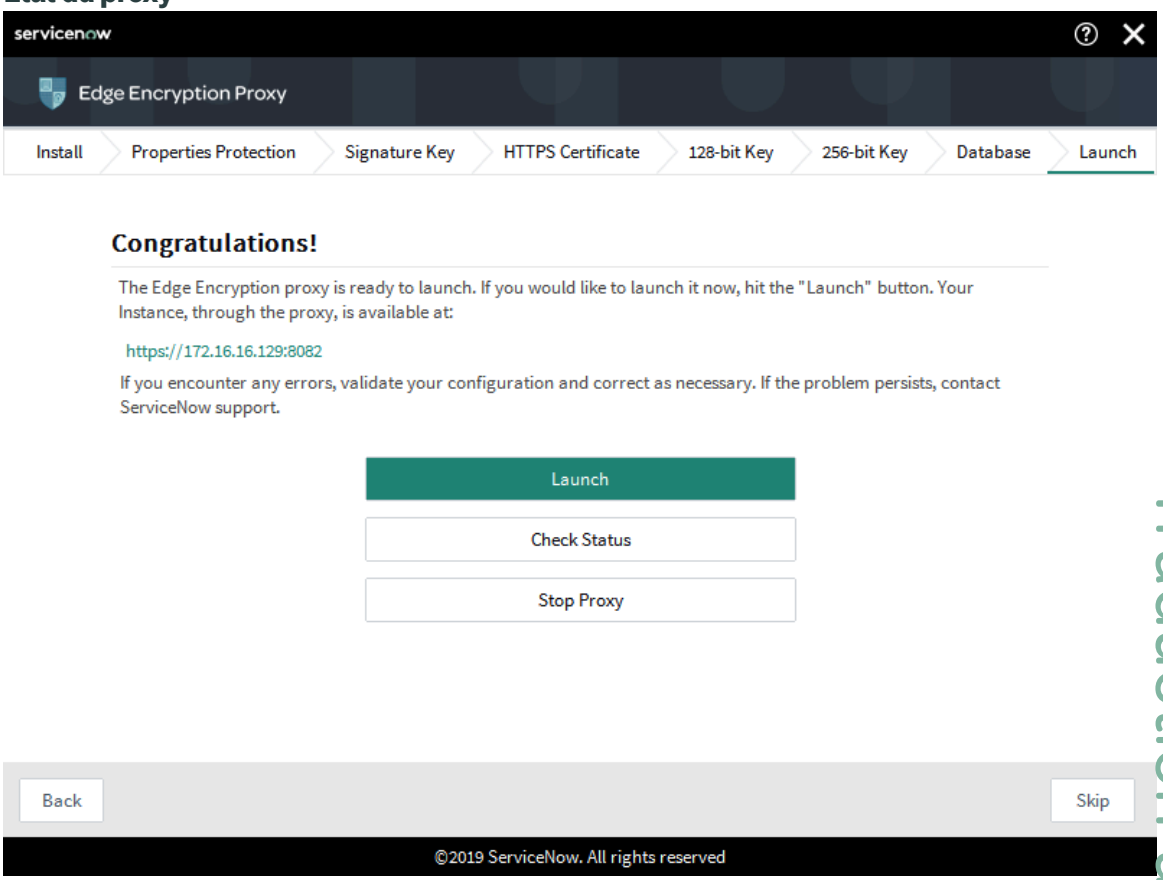
1. Après avoir configuré les clés sur l'instance et configuré la base de données proxy, revenez au programme d'installation du Chiffrement Edge proxy et cliquez sur **Lancer**.
2. Si un problème est détecté, ou pour vérifier l'état de votre serveur proxy, vous pouvez cliquer sur **Vérifier l'état** pour vérifier que le proxy est en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message affiche l'état du proxy.

État du proxy



Que faire ensuite

Après l'installation réussie du Chiffrement Edge serveur proxy, Définir la limite de mémoire initiale et la limite de mémoire de limite supérieure du serveur proxy.

Vérifier et dépanner l'installation du serveur proxy Chiffrement Edge

Une fois votre Chiffrement Edge proxy installé, vous pouvez vérifier l'installation pour localiser les problèmes ou démarrer et arrêter le proxy.

Avant de commencer

Rôle requis : admin

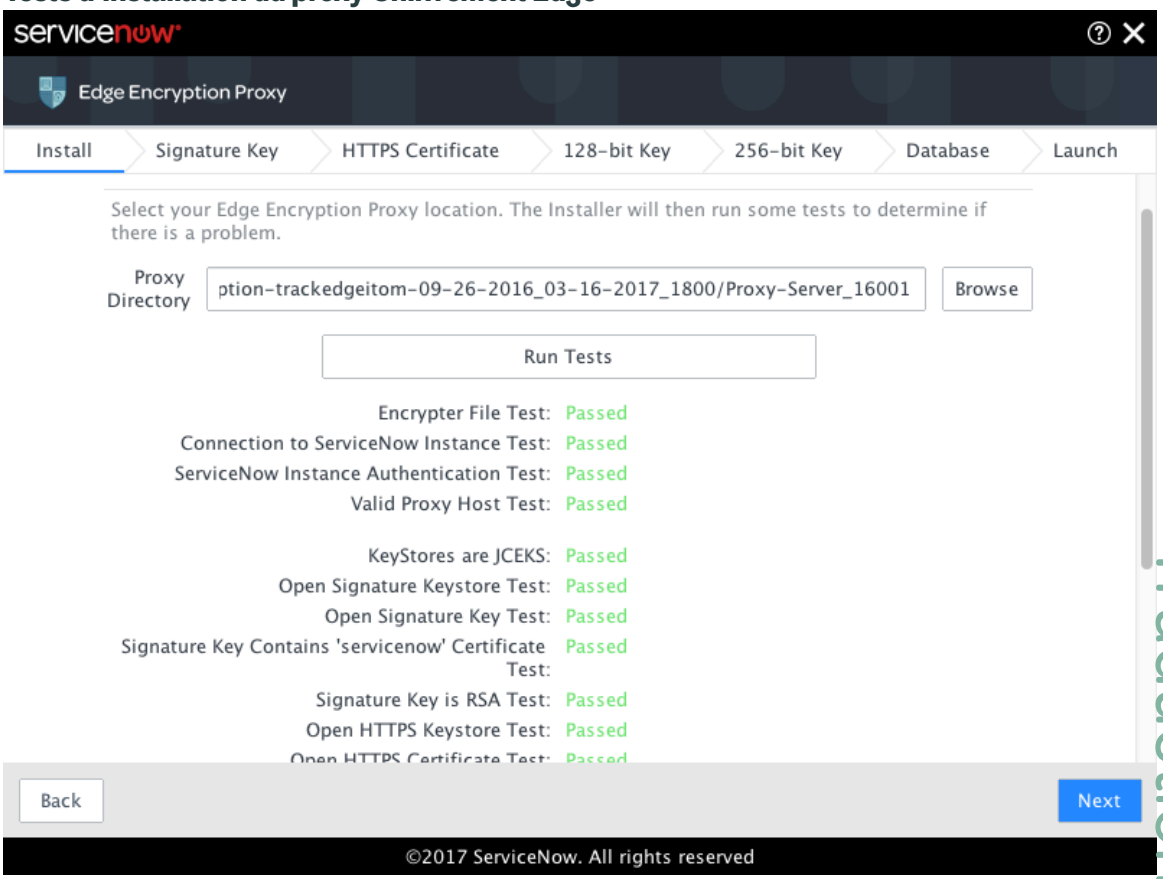
Procédure

1. Ouvrez le programme d'installation du Chiffrement Edge proxy.
2. Sélectionnez **Vérifier l'installation**.
3. Cliquez sur **Répertoire proxy** et sélectionnez le répertoire proxy.
4. Cliquez sur **Exécuter les tests**.
   Les résultats des tests s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests d'installation du proxy Chiffrement Edge



5. Cliquez sur **Suivant**.
   Si un problème est rencontré, vous pouvez parcourir le programme d'installation pour corriger la configuration. Si aucun problème n'est rencontré, le programme d'installation passe à la page **de lancement** . Vous pouvez vérifier l'état du proxy, arrêter le proxy ou démarrer le proxy à partir de la page **de lancement** .

Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande

Installez manuellement plusieurs Chiffrement Edge serveurs proxy dans votre réseau.

Avant de commencer

Rôles requis : security_admin sur votre ServiceNow instance et administrateur local sur l'ordinateur hôte.

Si des types de chiffrement ou des modèles de chiffrement préservant l'ordre doivent être utilisés, configurez une base de données MySQL sur une machine de votre réseau si elle n'est pas déjà présente.

Remarque :
Si vous utilisez les clés de chiffrement de la technologie Unbound avec Chiffrement Edge, installez le serveur proxy à l'aide du programme d'installation de ligne de commande sur l'ordinateur client Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Tout d'abord, configurez un seul Chiffrement Edge serveur proxy. Une fois que votre premier serveur proxy est en cours d'exécution, ajoutez des serveurs proxy supplémentaires pour une instance afin de garantir un environnement optimal. Reportez-vous à la section Dimensionnement de votre environnement Edge Encryption pour déterminer le nombre de serveurs proxy supplémentaires nécessaires.

Installer le serveur proxy Chiffrement Edge (programme d'installation de ligne de commande)

Installez un Chiffrement Edge proxy sur un ordinateur Windows ou Linux 64 bits.

Avant de commencer

Rôle requis : admin

La version Java 11.0.6 ou ultérieure de la série de versions 11.x est requise pour exécuter le programme d'installation.

Pourquoi et quand exécuter cette tâche

Installez le Chiffrement Edge serveur proxy sur un ordinateur de votre réseau à l'aide de la commande appropriée pour votre ordinateur cible. Si vous installez le Chiffrement Edge serveur proxy sur un ordinateur Windows, vous devez également installer le serveur proxy en tant que service Windows.

Lorsque vous mettez à niveau le serveur proxy Chiffrement Edge, le système sauvegarde l'ancien proxy dans le répertoire backup.dist-upgrade-<timestamp> sous le répertoire d'installation actuel. Le répertoire de sauvegarde est généré pendant le processus de mise à niveau et stocke les anciennes informations du proxy.

Lorsque vous exécutez une mise à niveau via la ligne de commande, une dist-upgrade.log peut être générée dans le répertoire où la commande s'exécute. La dist-upgrade.log contient des journaux pour le processus de mise à niveau.

En cas d'échec d'une mise à niveau, le système crée un répertoire failed-backup.dist-upgrade-<timestamp> . De plus, les journaux/wrapper.log dans le répertoire proxy d'origine peuvent également contenir des informations sur les défaillances.

Procédure

1. Créez le répertoire d'installation.
2. Téléchargez le fichier d'archive Chiffrement Edge proxy dans le répertoire d'installation.
3. Ouvrez le terminal et accédez au répertoire d'installation.

> **Remarque :**
> Si vous effectuez l'installation sur un ordinateur Windows, vous devez démarrer l'invite de commandes Windows avec les privilèges d'administrateur.

4. Exécutez cette commande pour la machine cible et modifiez les variables en fonction de votre configuration :
   `java -jar edgeencryption-<version>-all.jar -m install –n <proxy_name> --instancehost <host> -p <port> --protocol https –s <install_path>`

Option	Variable	Description
aucun	version	Numéro de version du Chiffrement Edge proxy utilisé pour effectuer l'opération en cours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Variable	Description
-m	Mode	Mode d'exécution. Les options sont « installer » pour un nouveau serveur proxy Edge ou « dist-upgrade » pour mettre à niveau un serveur proxy Edge existant.
-n	proxy_name	Nom du serveur proxy installé Chiffrement Edge . Utilisez une proxy_name unique pour pouvoir identifier des instances proxy spécifiques.
--instancehost	hôte	Le nom d'hôte de votre instance ServiceNow (par exemple, mycompany.service-now.com).
-p	port	Port sur lequel votre ServiceNow instance écoute. En général, les connexions HTTPS sécurisées écoutent sur le port **443** et les connexions HTTP écoutent sur le port **80**.
--protocole	protocol	Protocole utilisé par le proxy Edge installé lors de la connexion à l'hôte back-end ServiceNow . Il s'agit généralement **de HTTPS** (préféré pour les connexions TLS sécurisées) ou **HTTP** (connexions sans TLS) selon le protocole pris en charge par l'instance hôte.
-s	install_path	Chemin d'accès au répertoire ou au dossier où le nouveau proxy Edge est installé (répertoire de destination). Si le répertoire n'existe pas déjà, cette commande le créera. S'il existe, il ne doit pas contenir d'installation existante. Si cette option est ignorée, le nom de dossier par défaut est dérivé du proxy_name et du port (par exemple, EdgeProxy_443) dans le répertoire actuel.

Remarque :
Ne copiez pas et ne collez pas de commandes à partir du navigateur. Parfois, les opérations de copier/coller entraînent le collage de caractères inattendus sur la machine cible et entraînent une exécution incorrecte de la commande. Il est préférable de taper la commande à la main en utilisant la documentation comme référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher l'écran d'aide, exécutez cette commande avec l'option –aide : java -jar edgeencryption-<version>-all.jar --help

5. En cas d'installation sur un ordinateur Windows, installez le Chiffrement Edge proxy en tant que service Windows.

   a. **Facultatif :** Modifiez le nom du service en ouvrant le fichier conf/wrapper.conf sur le nouveau proxy et en définissant les propriétés dans la table suivante.

Propriété	Description
wrapper.ntservice.name	Nom unique du Chiffrement Edge service proxy.
Wrapper.NTSERVICE.DisplayName	Chiffrement Edge Nom d'affichage du service proxy.
wrapper.ntservice.description (facultatif)	Description du serveur proxy.

   Si cette étape n'est pas effectuée, le Chiffrement Edge service proxy est installé sous le nom de **Chiffrement Edge**.

   b. Enregistrez et fermez le fichier.

   c. Ouvrez l'invite de commande Windows et cd to ServerName_port/bin.

   d. Exécutez edgeencryption.bat installation.

Résultats

Le répertoire ProxyName_port est créé dans le répertoire actuel. Le fichier edgeencryption.properties est mis à jour avec les valeurs d'hôte, de port et de protocole de la ligne de commande.

Créer et configurer la paire de clés RSA pour la signature numérique

Créez une paire de clés RSA que le serveur proxy peut utiliser pour créer la signature numérique afin de signer les modifications apportées aux propriétés et à la configuration de chiffrement.

Avant de commencer

Rôle requis : admin

Pour générer et valider la signature numérique, une paire de clés RSA doit être générée et stockée dans le JCEKS Java KeyStore et chaque proxy doit être configuré pour utiliser cette paire de clés. Générez une paire de clés de chiffrement à l'aide de la commande keytool.

Pour utiliser l'utilitaire keytool avec un proxy installé sur SElinux (CentOS), vous devez activer le chargement des bibliothèques partagées à partir du répertoire java-installation proxy. Pour ce faire, exécutez la commande suivante en tant que root.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <proxy install dir>java/jre/bin/keytool.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez au répertoire KeyStore dans le répertoire de téléchargement proxy.
2. Changez le mot de passe par défaut.

   Le mot de passe par défaut est *changeme*.

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
   ```

3. Créez une paire de clés de chiffrement.

   Remarque :
   Ne saisissez pas de mot de passe pour la clé lorsque l'utilitaire keytool vous en demande un.

   Entrez cette commande sur une seule ligne.

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks
   -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. Mettez à jour le fichier de propriétés du proxy de chiffrement (edgeencryption.properties).

   a. Accédez au répertoire < installation >/conf/ .

   b. Ouvrez le fichier edgeencryption.properties .

   c. Entrez les propriétés de la signature numérique.

      Ces propriétés doivent être identiques pour tous les proxys.

5. Enregistrez et fermez le fichier edgeencryption.properties .

Importer et configurer le certificat pour la connexion SSL sécurisée

Pour utiliser une connexion SSL sécurisée, importez un certificat de serveur et ajoutez-le au Java KeyStore.

Avant de commencer

Rôle requis : admin

Vous devez obtenir le certificat du serveur et la clé privée correspondante avant de l'ajouter au Java KeyStore.

Procédure

1. Générez une demande de signature de certificat (CSR) à l'aide de la commande `openssl` .

   ```
   openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
   ```

2. Envoyez votre CSR (MYCSR.csr dans l'exemple ci-dessus) à votre autorité de certification pour le faire signer.
3. Créez un magasin de clés P12 pour l'importation à l'aide de la commande `openssl` .

   ```
   openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name shared >
    MY_SERVER.p12
   ```

4. Stockez votre certificat et votre clé privée dans un fichier jceks.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
 MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

L'alias, affiché dans l'exemple sous la forme MYALIAS , peut être n'importe quelle valeur. Vous utiliserez cet alias dans la propriété edgeencryption.proxy.https.cert.alias dans le fichier edgeencryption.properties situé dans le dossier <répertoire d'installation>/conf/ .

5. Arrêtez et redémarrez le proxy de périphérie.

Remarque :
Lors d'un redémarrage, le serveur proxy est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

Configurer un magasin de clés et des clés de chiffrement

Configurez le magasin de clés et les clés de chiffrement utilisés par le Chiffrement Edge serveur proxy.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Déterminez soigneusement le type de magasin de clés approprié à utiliser en fonction des besoins de votre organisation.

Magasin de clés pris en charge	Description
Magasin de fichiers	Les clés sont stockées dans un fichier dans un système de fichiers auquel le Chiffrement Edge serveur proxy accédait. Étant donné que les clés de chiffrement stockées dans un fichier ne sont pas chiffrées, il est de votre responsabilité de protéger ces fichiers.
Magasin de clés Java	Un KeyStore Java : ○ Stocke les clés dans un magasin de clés Java JCEKS. ○ Est protégé par un mot de passe et plus sécurisé que le stockage des clés dans un fichier dans le système de fichiers. ○ Peut stocker plusieurs clés. Un alias de clé représente chaque clé, ce qui facilite la gestion de plusieurs clés. Le Chiffrement Edge proxy est fourni avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier de magasin de clés contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow
Gestion des clés d'entreprise (EKM)	**SafeNet KeySecure** Les clés sont stockées et récupérées avec la gestion des clés SafeNet KeySecure. Vous devez obtenir une licence auprès de Gemalto , télécharger les bibliothèques et installer le magasin de clés SafeNet KeySecure sur une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Magasin de clés pris en charge	Description
	machine hôte de votre réseau avant de configurer le magasin de clés sur le Chiffrement Edge serveur proxy. **Technologie non liée** La clé de chiffrement encapsulée codée en base64 est stockée sous forme de fichier texte sur le Chiffrement Edge serveur proxy. L'implémentation de la technologie Unbound (anciennement Dyadic Security) conserve le contrôle de la clé d'encapsulation. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Remarque :
Si vous utilisez un magasin de clés autre que le magasin de clés Java JCEKS du système de base, vous devez importer la ServiceNow clé publique dans votre magasin de clés. L'alias de clé publique est *servicenow*.

2. Configurez le magasin de clés et les clés de chiffrement sur votre réseau local.

Configurer un magasin de clés Java KeyStore

Vous pouvez utiliser un magasin de clés Java KeyStore pour stocker les clés de chiffrement.

Avant de commencer
Rôle requis : admin

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <proxy install dir>/java/jre/bin/keytool.

Pourquoi et quand exécuter cette tâche
Le Chiffrement Edge proxy est fourni avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier de magasin de clés contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow

Procédure

1. Configurez les propriétés du magasin de clés.
   a. Accédez au répertoire < installation >/conf/ .
   b. Ouvrez le fichier edgeencryption.properties .
   c. Entrez les propriétés du KeyStore Java.
2. Enregistrez et fermez le fichier edgeencryption.properties .

Que faire ensuite
Après avoir configuré le KeyStore Java, Créer des clés de chiffrement à l'aide du keytool Java KeyStore.

Créer des clés de chiffrement à l'aide du keytool Java KeyStore

Vous pouvez utiliser l'outil clé fourni avec la distribution proxy de chiffrement pour créer des clés de chiffrement AES 128 bits et AES 256 bits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <proxy install dir>/java/jre/bin/keytool.

Pour en savoir plus sur l'utilitaire keytool, consultez la documentation Java SE .

Pourquoi et quand exécuter cette tâche

Remarque :
Le Java KeyStore exige que le nom de l'alias (nom de clé, alias de clé) utilise des lettres minuscules et des chiffres.

Procédure

1. Accédez au répertoire keystore, <répertoire d'installation>/keystore/.
2. Pour créer la clé de chiffrement, exécutez l'une des commandes suivantes.

Remarque :
Si vous choisissez d'exécuter ces commandes à partir d'un répertoire autre que le répertoire du magasin de clés, c'est-à-dire que vous avez ignoré l'étape précédente, vous devez modifier l'option *-keystore* pour inclure le chemin de votre répertoire actuel vers le répertoire du magasin de clés. Par exemple, si vous étiez dans le répertoire <installation>\bin , l'option serait `-keystore .. /keystore/keystore.jceks`.

Option	Description
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Vous ajoutez l'alias sur l'instance lorsque vous affectez des clés par défaut.

Remarque :
Le mot de passe de clé doit être identique à celui du magasin de clés.

Configurer un magasin de clés SafeNet KeySecure

Si vous utilisez un magasin de clés SafeNet, copiez un ensemble de bibliothèques dans le répertoire de distribution proxy.

Avant de commencer
Rôle requis : admin

Vous devez installer et configurer le magasin de clés SafeNet avant d'effectuer cette étape. Obtenez une licence auprès de Thales afin de télécharger les bibliothèques.

Remarque :
Pour la version 8.12 d'IngrianNAE, vous devez également télécharger le fichier commons-collections.jar

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Remarque :
Sous Linux, les chemins d'accès aux fichiers utilisent une barre oblique (/).

Procédure

1. Accédez au répertoire <installation>/conf/ et ouvrez le fichier edgeencryption.properties .
2. Entrez les propriétés du magasin de clés SafeNet.

Remarque :
Vous pouvez configurer le magasin de clés SafeNet à l'aide de l'authentification par nom d'utilisateur/mot de passe ou authentification par certificat client, mais pas une combinaison des deux.

Example

Exemple d'un magasin de clés SafeNet utilisant l'authentification par nom d'utilisateur et mot de passe.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Exemple de magasin de clés SafeNet utilisant l'authentification par certificat client. Cette méthode d'authentification élimine la nécessité de stocker le nom d'utilisateur et le mot de passe du serveur SafeNet dans le fichier de propriétés.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. Ajoutez ou créez une clé dans le magasin de clés SafeNet.
   Vous ajoutez le nom de la clé (alias) sur l'instance lorsque vous affectez des clés par défaut.
4. Enregistrez et fermez le fichier edgeencryption.properties .

Surclassement de Kingston ou version antérieure vers London ou supérieur

Si vous utilisez un serveur NAE SafeNet pour le stockage de clés avec Edge, avant de mettre à niveau le proxy vers une version antérieure London ou supérieure, vous devez copier les fichiers JAR ProtectApp Kingston du client Gemalto SafeNet et ajouter de nouvelles propriétés.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Remarque :
Sous Linux, les chemins d'accès aux fichiers utilisent une barre oblique (/).

Procédure

1. Copiez les fichiers suivants de <répertoire d'installation>/lib dans le répertoire <install>/nae :
   - commons-collections<version>.jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<version>.jar
2. Sur la version actuelle (non mise à niveau) du proxy, mettez à jour le fichier <répertoire d'installation>/conf/edgeencryption.properties en ajoutant les deux propriétés suivantes :
   - *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   - *edgeencryption.thirdparty.vendor.library.path* = <chemin d'accès au répertoire dans lequel vous avez copié les fichiers jar à l'étape 1>

     Remarque :
     edgeencryption.thirdparty.vendor.library.path pour Java 11.
3. Enregistrez les changements.
4. Procédez à la mise à niveau vers London ou vers une version supérieure.

Configurer les clés de technologie Unbound

Utilisez les clés de la technologie Unbound (anciennement Sécurité dyadique) en Chiffrement Edge stockant la clé de chiffrement enveloppée encodée en base64 sous forme de fichier texte sur le Chiffrement Edge serveur proxy et en fournissant l'alias de clé d'encapsulation. L'implémentation de la technologie Unbound conserve le contrôle de la clé d'encapsulation.

Avant de commencer

Rôle requis : security_admin

Dans votre implémentation Unbound Technology, identifiez à la fois la clé d'encapsulation et la clé encapsulée. Utilisez l'algorithme RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING pour l'emballage et le remplissage. Exporter la clé encapsulée au format texte codé en base64. Enregistrez le fichier à l'aide de l'alias de clé comme nom sans extension de fichier.

Remarque :
Si vous utilisez les clés de chiffrement de la technologie Unbound avec Chiffrement Edge, installez le serveur proxy à l'aide du programme d'installation de ligne de commande sur l'ordinateur client Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Procédure

1. Ajoutez la clé de chiffrement encapsulée au format texte codé base64 au répertoire <proxy-installation-directory>/keys .
   Le nom du fichier doit être l'alias de clé sans extension de fichier.
2. Mettez à jour le fichier edgeencryption.properties .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez au répertoire <proxy-installation-directory>/conf .

b. Ouvrez le fichier edgeencryption.properties .

c. Entrez les propriétés du magasin de fichiers et définissez la valeur de `edgeencryption.keyfile.directory` to keys.

   Cette propriété demande au serveur proxy de rechercher la clé de chiffrement dans le répertoire <Java-home-directory>/keys .

   Pour plus d'informations sur Chiffrement Edge les propriétés, consultez Propriétés du serveur proxy Chiffrement Edge.

d. Décommentez les propriétés pour la configuration du fournisseur dyadique et définissez la valeur de l'alias de `edgeencryption.ekm.provider.rsa.wrapping.key.alias` clé d'encapsulation dans votre implémentation Unbound.

e. Enregistrez et fermez le fichier.

Que faire ensuite

Ajoutez l'alias de clé de chiffrement à l'instance. L'alias de clé de chiffrement est le nom de fichier de la clé de chiffrement enveloppée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier dans le répertoire est nommé myunboundkey, ajoutez ce nom au champ **Alias de clé** . Reportez-vous à Configurer les clés de chiffrement sur l'instance.

Créer une clé de chiffrement stockée dans un fichier

Vous pouvez utiliser un simple fichier texte comme magasin de clés. Chaque fichier contient une clé de chiffrement unique.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Cette étape crée à la fois le stockage de clés et la clé de chiffrement.

Remarque :
Le nom du fichier de clé doit correspondre à l'alias de clé spécifié dans la table des clés de chiffrement de l'instance. Voir Configurer les clés de chiffrement sur l'instance.

Procédure

1. Créez un fichier dans le dossier /keys du répertoire d'installation du serveur proxy.
2. Ajoutez la clé de chiffrement au fichier.

Option	Description
AES 128	Placez la clé de chiffrement, exactement 16 octets, dans le fichier.
AES 256	Placez la clé de chiffrement, exactement 32 octets, dans le fichier.

3. Mettez à jour le fichier edgeencryption.properties .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez au répertoire < installation >/conf/ .

b. Ouvrez le fichier edgeencryption.properties .

c. Entrez les propriétés du magasin de fichiers.

d. Enregistrez et fermez le fichier.

Configurer les clés de chiffrement sur l'instance

Chiffrement Edge fournit les outils permettant de gérer les clés de chiffrement sans mettre le proxy hors ligne.

Avant de commencer

Rôle requis : security_admin

Avant de configurer de nouvelles clés de chiffrement sur l'instance :

1. Créez la clé de chiffrement.
2. Mettez la nouvelle clé à la disposition de tous les proxys de chiffrement. Copiez le fichier ou le fichier Java KeyStore sur chaque proxy ou assurez-vous que chaque proxy a accès au périphérique Java KeyStore ou à l'appareil de gestion des clés d'entreprise (EKM).

Pourquoi et quand exécuter cette tâche

Les alias de clés doivent être uniques. Chaque alias de clé doit avoir la même taille et le même type de clé sur chaque proxy, sinon la clé ne peut pas être affectée par défaut.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Configurer les clés.**.
2. Dans la section Ajouter de nouvelles clés du formulaire, procédez comme suit pour ajouter une nouvelle clé.

> **Important :**
> Si vous utilisez des clés versionnées SafeNet, une colonne supplémentaire s'affiche pour la version de la **clé**. La **version de la clé** ne peut pas être modifiée. Cliquez sur le lien **Récupérer les dernières versions de clé** dans les liens connexes pour récupérer la dernière version de chaque clé à partir du proxy Edge.

Les lignes de la liste avec un **X** dans la colonne de gauche peuvent être supprimées. Les clés qui ont été utilisées par défaut ou qui ont un **étatdisponible** ne peuvent pas être supprimées.

a. Double-cliquez sur la ligne qui indique **Insérer une nouvelle ligne.**

b. Dans la zone d'édition, saisissez un nom pour la clé, puis cliquez sur la coche.

Les alias clés sont des lettres minuscules et des chiffres. Les lettres majuscules sont remplacées par des lettres minuscules lorsque vous cliquez sur **Mettre à jour**. Les alias de clés doivent être uniques.

> **Remarque :**
> Si vous utilisez des clés technologiques Unbound, ajoutez l'alias de clé de chiffrement. L'alias de clé de chiffrement est le nom de fichier de la clé de chiffrement enveloppée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier dans le répertoire est nommé myunboundkey, ajoutez ce nom au champ **Alias de clé** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sur la même ligne, double-cliquez dans la colonne Taille de la **clé** .

d. Dans la zone de sélection, sélectionnez une taille de clé, **128 bits** ou **256 bits**, puis cliquez sur la coche.

e. Sur la même ligne, double-cliquez dans la colonne **Type** .

f. Dans la zone de sélection, sélectionnez un type de clé, soit **Fichier**, **Keystore**, **SafeNet** ou **Unbound**, puis cliquez sur la coche.

g. Lorsque vous avez terminé d'ajouter des clés, cliquez sur **Étape suivante**.
Vous devez spécifier un alias, une taille de clé et un type de clé pour chaque clé avant de continuer.

3. Dans la section État des clés du formulaire, vérifiez **l'état** de la clé et assurez-vous qu'elle est **disponible**.
4. Lorsque la clé est **disponible**, cliquez sur **Étape suivante**.
Cette opération peut prendre quelques minutes.

Remarque :
Si vous utilisez des clés versionnées SafeNet, une colonne supplémentaire s'affiche pour la version de la **clé**. La **version de la clé** ne peut pas être modifiée.

L'instance suit l'état de chaque clé de chiffrement disponible pour n'importe quel proxy. Lorsqu'une clé est disponible sur tous les proxys, son état devient **Disponible**. Si l'état ne change pas après quelques minutes, vérifiez que la clé est disponible sur tous les proxys. Si l'état reste **Indisponible**, un ou plusieurs proxys n'ont pas la clé.

États des clés de chiffrement

États	Description
Disponible	Tous les proxys en ligne ont la clé.
Non disponible	Il s'agit d'une nouvelle clé et les proxys n'ont pas encore chargé la clé, ou au moins un proxy n'a pas réussi à charger la clé.

5. Dans la section Modifier les clés par défaut du formulaire, effectuez l'une des actions suivantes :
   - Saisissez l'alias de la clé.
   - Cliquez sur l'icône de loupe et sélectionnez un alias.

Remarque :
Si vous utilisez des clés versionnées SafeNet, un champ supplémentaire s'affiche pour la version de la **clé**. La **version de la clé** est grisée et ne peut pas être modifiée. Choisissez uniquement la version de clé la plus récente. Si vous choisissez une version antérieure, le message suivant s'affiche lorsque vous cliquez sur **Mettre à jour** ou **Étape suivante**.

```
One of the default keys chosen is not the latest version available for the key. Please use the latest version.
```

Si les clés par défaut ne correspondent pas aux dernières versions des clés SafeNet, un lien Mettre **à jour les clés par défaut vers la dernière version** s'affiche dans les liens connexes. Cliquez sur le lien pour mettre à jour les clés par défaut afin d'utiliser la dernière version.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la section Planifier la rotation de clé du formulaire, planifiez une tâche de rotation de clé en masse ou une tâche de rotation de clé unique pour chiffrer les données existantes à l'aide de la nouvelle clé de chiffrement.

   Si vous n'exécutez pas de tâche de rotation de clé en masse ou de tâche de rotation de clé unique, les données existantes restent chiffrées avec l'ancienne clé jusqu'à ce que vous puissiez accéder à nouveau aux données.

Configurer des propriétés supplémentaires dans le fichier de propriétés de Chiffrement Edge

Après avoir installé le Chiffrement Edge serveur proxy dans votre réseau et configuré votre magasin de clés et vos clés, configurez les propriétés supplémentaires Chiffrement Edge .

Avant de commencer
Rôle requis : admin

Procédure

1. Ouvrez le fichier <répertoire d'installation>/conf/edgeencryption.properties et configurez les propriétés de serveur proxy suivantes Chiffrement Edge :
   - Propriétés cibles (instance)
   - Propriétés du compte utilisateur
   - Propriétés de proxy
   - Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, configurez les propriétés de la base de données du proxy
   - Texte clair et propriétés IV statiques
2. Enregistrez et fermez le fichier.

Configurer un proxy web

Si votre réseau utilise un proxy web, vous pouvez configurer le Chiffrement Edge proxy pour utiliser le proxy web.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Si votre réseau n'utilise pas de proxy web, laissez les propriétés du proxy web dans le fichier de configuration commentées.

Le Chiffrement Edge serveur proxy prend en charge la connexion HTTP et l'authentification de base avec le proxy web.

Procédure

1. Accédez au répertoire < installation >/conf/ .
2. Ouvrez le fichier edgeencryption.properties .
3. Configurez les propriétés du proxy web.
4. Enregistrez et fermez le fichier edgeencryption.properties .
5. Si le proxy web utilise un certificat de serveur spécifique au client, ajoutez ce certificat à la JVM utilisée par le serveur proxy pour établir la Chiffrement Edge confiance entre le proxy web et le Chiffrement Edge serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Utilisez la commande `cd` pour accéder au <répertoire de base Java>/jre/lib/security/cacerts

b. Exécutez la commande : `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>`

Définir la limite de mémoire initiale et la limite de mémoire de limite supérieure du serveur proxy

Définissez la limite de mémoire initiale et la limite de mémoire de limite supérieure pour spécifier la quantité de mémoire que le serveur proxy peut consommer. Définissez ces limites pour éviter les problèmes de performances dans votre Chiffrement Edge implémentation.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
À titre indicatif, définissez la limite de mémoire initiale et la limite de mémoire de limite supérieure sur la même valeur. Sur n'importe quelle machine, allouez 2 Go de mémoire physique au système d'exploitation (OS). Ensuite, allouez le reste de la mémoire physique au tas en utilisant les propriétés de limite de mémoire initiale et de limite de mémoire de limite supérieure. Par exemple, sur un ordinateur avec 8 Go de mémoire, allouez 2 Go au système d'exploitation et allouez les 6 Go restants (6144 m) à la mémoire initiale et à la mémoire de limite supérieure.

Important :
Si votre Chiffrement Edge serveur proxy est en cours d'exécution, vous devez arrêter et redémarrer le serveur proxy après la mise à jour de ces propriétés.

Procédure

1. Dans le répertoire de votre serveur proxy, ouvrez <rép d'installation>/conf/wrapper.conf.

2. Pour définir la limite de mémoire initiale, ajoutez la ligne suivante à la fin du fichier :

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```

Définissez `<number>` au `prochain <number>` disponible dans la séquence des propriétés `wrapper.java.additional.<number>` définies dans le fichier `wrapper.conf` .

Example
Par exemple, vous avez la liste suivante de propriétés `wrapper.java.additional.<number>` :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Le `<nombre>` maximum dans la liste ci-dessus est **de 2**. Lorsque vous ajoutez la ligne `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` , définissez `<number>` sur **3**, le prochain nombre disponible.

Important :
Ne laissez pas d'espaces dans la séquence de numérotation.

Définissez `<min_memory_in_MB>` sur le nombre de mégaoctets de mémoire restants après avoir alloué 2 Go de mémoire au système d'exploitation.

3. Définissez la limite de mémoire de la limite supérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comme une limite de mémoire de limite supérieure n'est pas définie dans le système de base, le serveur proxy peut utiliser toute la mémoire disponible. Si d'autres services sont en cours d'exécution sur le serveur, vous pouvez définir la limite de mémoire de limite supérieure.

Ajoutez la ligne suivante à la fin du fichier :

`wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m`

Définissez `<number>` au `prochain <number>` disponible dans la séquence des propriétés `wrapper.java.additional.<number>` définies dans le fichier `wrapper.conf` .

Example

Par exemple, vous avez la liste suivante de propriétés `wrapper.java.additional.<number>` :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Le `<nombre>` maximum dans la liste ci-dessus est **de 2**. Lorsque vous ajoutez la ligne `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m` , définissez `<number>` sur **3**, le prochain nombre disponible.

Remarque :
Ne laissez pas d'espaces dans la séquence de numérotation.

Définissez `<max_memory_in_MB>` sur le nombre de mégaoctets de mémoire restants après avoir alloué 2 Go de mémoire au système d'exploitation.

4. Enregistrez et fermez le fichier.

Example: Exemple : Définition des limites de mémoire initiale et supérieure du serveur proxy

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Que faire ensuite

Démarrer le proxy Chiffrement Edge.

Démarrer le proxy Chiffrement Edge

Une fois qu'un Chiffrement Edge proxy est installé et configuré, vous pouvez le démarrer à partir de la ligne de commande.

Avant de commencer

Rôle requis : admin

Avant de démarrer le proxy de chiffrement, vérifiez les points suivants :

- Le Chiffrement Edge module d'extension est activé sur l'instance.
- Le fichier edgeencryption.properties sur cet ordinateur a été configuré.
- Si vous utilisez un ordre préservant le type de chiffrement ou les modèles de chiffrement, la base de données proxy est en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
La première fois que vous configurez le fichier edgeencryption.properties ou que vous modifiez les propriétés, vous ne souhaitez peut-être pas définir la propriété de chiffrement par mot de passe. Après avoir vérifié que tout fonctionne, vous pouvez définir la propriété de cryptage du mot de passe, arrêter le proxy, puis redémarrer le proxy.

Procédure

1. Exécutez le serveur proxy.

Option	Description
Sur un ordinateur Linux	**a.** cd à ServerName_port **b.** Exécuter ./startup.sh
Sur un ordinateur Windows	Effectuez les étapes suivantes à partir de la ligne de commande en tant qu'administrateur : **a.** CD vers ServerName_port/BIN **b.** Exécuter edgeencryption.bat début

2. Vérifiez le journal sur le serveur proxy pour vérifier que le proxy est en cours d'exécution.

Grisez les mots de passe dans le fichier de propriétés

Grisez les mots de passe dans le fichier edgeencryption.properties pour pouvoir partager le fichier de propriétés sans révéler de mots de passe en texte clair.

Avant de commencer
Rôle requis : admin

Assurez-vous que le serveur proxy est configuré et en cours d'exécution Chiffrement Edge avant de définir cette propriété. Avant de définir cette propriété, Arrêter le proxy Edge Encryption..

Pourquoi et quand exécuter cette tâche
La définition de cette propriété peut rendre difficile le débogage des problèmes de connexion et d'accès lors du démarrage initial. Définissez cette propriété uniquement dans les environnements de production une fois que le proxy a été configuré et testé avec succès.

Procédure

1. Accédez au répertoire < installation >/conf/ .
2. Dans le répertoire conf , créez un fichier texte contenant une chaîne ou une phrase complexe qui peut être utilisée comme phrase de sécurité que le proxy utilise pour obscurcir les mots de passe dans le fichier edgeencryption.properties .
   Cette phrase de passe doit être une phrase aléatoire et complexe sans rapport avec les mots de passe eux-mêmes.
3. Ouvrez le fichier edgeencryption.properties .
4. Définissez la propriété de chiffrement du mot de passe.
5. Enregistrez et fermez le fichier edgeencryption.properties .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Après avoir défini cette propriété, vous pouvez Démarrer le proxy Chiffrement Edge.

Ajouter manuellement un proxy supplémentaire

Une fois que le premier Chiffrement Edge proxy est correctement configuré et testé, vous pouvez configurer des proxys supplémentaires sur un ordinateur Linux ou Windows. Il n'est pas recommandé d'installer plusieurs proxys sur le même ordinateur.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ajoutez des serveurs proxy supplémentaires sur des machines supplémentaires pour garantir un environnement optimal. Reportez-vous à la section Dimensionnement de votre environnement Edge Encryption pour déterminer le nombre de proxys supplémentaires nécessaires.

Remarque :
Assurez-vous que tous les proxys ont les mêmes clés de chiffrement et la même paire de clés RSA utilisées pour signer numériquement la configuration de chiffrement et les règles de chiffrement. Si une base de données proxy a été configurée dans le cadre de l'installation, tous les proxys doivent utiliser la même base de données proxy.

Procédure

1. Installez le proxy à l'aide de la commande appropriée.
   Pour plus d'informations, consultez Installer le Chiffrement Edge serveur proxy (programme d'installation interactif).
2. Copiez toutes les clés de chiffrement et le fichier `edgeencryption.properties` du premier proxy vers le nouveau proxy.
   Les clés de chiffrement peuvent se trouver dans le magasin de clés proxy, dans le répertoire `/keys` ou dans un magasin de clés SafeNet KeySecure.
3. Ouvrez le fichier `edgeencryption.properties` sur le nouveau proxy.
4. Modifiez les propriétés suivantes :

Propriété	Description
edgeencryption.proxy.name	Nom unique du serveur proxy
edgeencryption.proxy.host	Nom du serveur, adresse IP ou nom de domaine complet de l'ordinateur exécutant le proxy.
edgeencryption.proxy.http.port	Port sur le proxy pour la communication HTTP. Doit être unique pour tous les processus sur l'ordinateur.
edgeencryption.proxy.https.port	Port sur le proxy pour la communication HTTPS. Doit être unique parmi les processus sur l'ordinateur.

5. Si vous installez le serveur proxy sur un ordinateur Windows, vous devez modifier le nom du service. En ouvrant le fichier `conf/wrapper.conf` sur le nouveau proxy et en ajoutant les propriétés répertoriées dans le tableau suivant.

Remarque :
Vous devez effectuer cette étape avant de lancer le serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
wrapper.ntservice.name	Nom unique du Chiffrement Edge service proxy.
wrapper.ntservice.displayname	Chiffrement Edge Nom d'affichage du service proxy.
wrapper.ntservice.description (Facultatif)	Description du serveur proxy.

6. Enregistrez et fermez le fichier.
7. Lancez le proxy à l'aide de la commande appropriée.
   Pour plus d'informations, consultez Démarrer le proxy Chiffrement Edge.

Authentifier un Chiffrement Edge serveur proxy

Spécifiez qu'un serveur proxy est une source fiable afin de Chiffrement Edge pouvoir traiter les demandes provenant de ce serveur proxy.

Avant de commencer

Si un serveur proxy n'est pas authentifié, le journal de la console inclut le message suivant :

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

Si vous tentez d'accéder au proxy, vous recevez le message suivant : `Ce site est inaccessible`.

Pour maintenir le proxy dans un état opérationnel pendant le processus de mise à niveau, l'authentification n'est pas requise tant que la mise à jour du proxy n'est pas réussie.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Proxys**.
2. Sélectionnez le proxy et cliquez sur **Authentifier**.

Résultats

Le proxy passe de **Non authentifié** à **En attente** puis **Authentifié**. L'état passe de **Non authentifié** à **En attente** lorsque vous démarrez l'authentification. Une fois l'authentification terminée, l'état passe de **En attente** à **Authentifié**. Vous pouvez accéder au proxy et Chiffrement Edge accepter les demandes du proxy.

Remarque :
Si vous arrêtez et redémarrez le proxy, celui-ci reste **authentifié** et redémarre avec succès.

Arrêter le proxy Edge Encryption.

Vous pouvez arrêter un Chiffrement Edge proxy à partir de la ligne de commande.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Arrêtez le serveur proxy.

Option	Description
Sur un ordinateur Linux	Exécuter `./shutdown.sh`
Sur un ordinateur Windows	Exécuter `edgeencryption.bat arrêter` Pour supprimer le service Windows, exécutez `edgeencryption.bat supprimer`

2. Vérifiez le journal sur le serveur proxy pour vérifier que le proxy s'est arrêté.

Désinstaller le proxy Chiffrement Edge sur Linux

Vous pouvez désinstaller le Chiffrement Edge proxy. Si vous mettez à niveau le proxy, il n'est pas nécessaire d'arrêter et de désinstaller la version actuelle.

Avant de commencer

Rôle requis : admin

Vous devez avoir accès à l'ordinateur exécutant le Chiffrement Edge proxy.

Pourquoi et quand exécuter cette tâche

Avant d'arrêter le Chiffrement Edge proxy, assurez-vous qu'aucun utilisateur n'est connecté à l'instance à l'aide du proxy.

Le proxy de chiffrement exécuté sous Linux fonctionne comme un processus unique. Vous pouvez terminer ce processus pour prendre en charge des tâches telles que le redéploiement du proxy de chiffrement sur un autre ordinateur hôte, la mise à jour de la version du proxy, la mise à jour de la version Java ou la modification du nom unique du proxy de chiffrement lors du déploiement du proxy de chiffrement sur plusieurs serveurs proxy.

Procédure

1. Vous pouvez enregistrer le fichier `edgeencryption.properties` avant de supprimer le répertoire de distribution.
2. Exécutez le script `shell shutdown.sh` .
3. Vérifiez le journal sur le serveur proxy pour vérifier que le serveur proxy est arrêté.
4. Supprimez les fichiers dans le dossier de distribution.

Désinstaller le proxy Chiffrement Edge sur Windows

Vous pouvez désinstaller le Chiffrement Edge proxy. Si vous mettez à niveau le proxy, il n'est pas nécessaire d'arrêter et de désinstaller la version actuelle.

Avant de commencer

Rôle requis : admin

Vous devez avoir accès à l'ordinateur exécutant le Chiffrement Edge proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant d'arrêter le Chiffrement Edge proxy, assurez-vous qu'aucun utilisateur n'est connecté à l'instance à l'aide du proxy.

Procédure

1. Vous pouvez enregistrer le fichier edgeencryption.properties avant de supprimer le répertoire de distribution.
2. Exécuter `edgeencryption.bat arrêter`
3. Exécuter `edgeencryption.bat supprimer`
4. Vérifiez le journal sur le serveur proxy pour vérifier que le serveur proxy est arrêté.
5. Supprimez les fichiers dans le dossier de distribution.

Configurer l'authentification unique (SSO) de plusieurs fournisseurs avec Chiffrement Edge

Configurez l'authentification unique (SSO) de plusieurs fournisseurs pour activer la connexion via l'URL du serveur proxy ou l'URL Chiffrement Edge de l'instance. Si vous implémentez l'authentification unique (SSO) de plusieurs fournisseurs avec Chiffrement Edge l'option activée, certains utilisateurs peuvent avoir besoin de se connecter à votre instance via le serveur proxy, tandis que d'autres Chiffrement Edge utilisateurs peuvent ne pas le faire.

Avant de commencer

- Activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).
- Activez le module d'extension Chiffrement Edge (com.glide.edgeencryption) et assurez-vous qu'un ou plusieurs serveurs proxy sont configurés dans votre réseau.
- Déterminez l'URL du serveur proxy via lequel les Chiffrement Edge utilisateurs se connecteront à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs. Pour déterminer l'URL d'un Chiffrement Edge serveur proxy, reportez-vous à la section Installation de Chiffrement Edge.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'utilisateur qui se connecte devra utiliser l'URL appropriée pour se connecter, soit en utilisant le proxy Edge, soit en ne l'utilisant pas.

- Si vous acheminez tous les utilisateurs via le Chiffrement Edge serveur proxy, configurez votre enregistrement d'identification de fournisseur et définissez l'URL du serveur proxy dans les champs Page **d'accueil de ServiceNow**, **ID d'entité/Émetteur** et **URI de l'audience** .
- Pour acheminer certains utilisateurs via le serveur proxy et d'autres utilisateurs vers l'instance, créez deux enregistrements de fournisseur d'identification. Les deux enregistrements utilisent la même valeur dans le champ **URL du fournisseur d'identité** . Toutefois, l'un des enregistrements est acheminé via le serveur proxy, tandis que l'autre est acheminé vers l'instance.
  - Connectez-vous via le nom d'instance : https://<nom d'instance>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id de l'enregistrement IdP pour le proxy non-Edge
  - Connectez-vous via le proxy Edge : https://<nom d'hôte Edge> :<port>/login_with_sso.do ?glide_sso_id=<sys_id de l'enregistrement IdP pour le proxy Edge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Activez la duplication des URL des fournisseurs d'identité dans les enregistrements des fournisseurs d'identité.
   Une contrainte unique empêche la duplication de l'URL du fournisseur d'identité dans deux enregistrements de fournisseur d'identité différents. Vous pouvez activer la duplication de l'URL du fournisseur d'identité dans plusieurs enregistrements IdP en définissant un champ sur faux.
   a. Accédez à la **Définition du système** > **Dictionnaire**.
   b. Ouvrez l'enregistrement de définition pour le champ **IdP** dans la table Fournisseurs d'identité [saml2_update1_properties].
   c. Configurez le formulaire pour ajouter le champ **Unique** .
   d. Assurez-vous que la valeur du champ **Unique** est définie sur **faux**.
2. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
3. Créez deux enregistrements de fournisseur d'identité pour le même fournisseur d'identité : l'un à l'aide de l'URL d'instance et l'autre à l'aide de l'URL du Chiffrement Edge serveur proxy.
   Pour créer un enregistrement de fournisseur d'identité, consultez Créer un fournisseur d'identité externe.
   a. Pour l'URL du Chiffrement Edge serveur proxy, remplissez le formulaire en utilisant ces valeurs.

Champ	Valeur
URL du fournisseur d'identité	Importé à partir des métadonnées IdP.
ServiceNow Page d'accueil	URL de la page d'accueil de votre serveur proxy. Par exemple : https://<nom d'hôte proxy> :<port>/navpage.do
ID d'entité/Émetteur	https://<nom d'hôte proxy> :<port>
URI de l'audience	https://<nom d'hôte proxy> :<port>

   b. Cliquez sur **Envoyer**.
   c. Pour l'URL de l'instance, remplissez le formulaire en utilisant ces valeurs.

Champ	Valeur
URL du fournisseur d'identité	Importé à partir des métadonnées IdP.
ServiceNow Page d'accueil	https://<instance>.service-now.com/navpage.do
ID d'entité/Émetteur	https://<instance>.service-now.com/navpage.do
URI de l'audience	https://<instance>.service-now.com/navpage.do

   d. Cliquez sur **Envoyer**.
4. **Facultatif :** Si vous utilisez plusieurs fournisseurs d'identité, modifiez la sortie de l'installation MultiSSO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Définition du système** > **Sorties d'installation**.
Le système affiche la liste actuelle des sorties d'installation.

b. Ouvrez la sortie d'installation **de l'authentification unique (SSO) à fournisseurs multiples** .

c. Recherchez l'instruction suivante dans le champ **Script** .

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
   }
}
```

d. Remplacez l'instruction par le code suivant.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
  /* // You have two profiles that use the same IdP entity id it cannot use
  // the IdP issuer / entity id from the response otherwise it may result in the
  // wrong IdP profile. IdP initiated login will not work
  var idpRecord = this.getIdPRecord(request);
  if (idpRecord) {
    SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
    return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
    }*/
  return new SSO_Helper(null, true);
  }
```

Remarque :
La connexion initiée par l'IdP ne fonctionne pas dans cette configuration.

e. Cliquez sur **Mettre à jour**.

5. Facultatif : Si vous utilisez plusieurs sociétés, configurez les utilisateurs pour l'authentification unique (SSO) de plusieurs fournisseurs et mettez à jour sys_id de l'enregistrement du fournisseur d'identité en fonction de l'utilisateur.

(Optional) Pour plus d'informations, consultez Configurer les utilisateurs pour l'authentification unique (SSO) de plusieurs fournisseurs.

- Pour configurer un utilisateur afin qu'il se connecte via le Chiffrement Edge serveur proxy, utilisez le sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL du Chiffrement Edge serveur proxy.
- Pour configurer un utilisateur afin qu'il se connecte à l'instance, utilisez le sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

URL de connexion

URL	Destination de la connexion
https://<nom d'hôte proxy> :<port>/ login_with_sso.do ?glide_sso_id=<sys_id de l'enregistrement IdP pour l'URL du serveur proxy>	Se connecte via le serveur proxy.
https://<nom d'instance>.service-now.com/ login_with_sso.do?glide_sso_id=<sys_id de l'enregistrement IdP pour l'URL de l'instance>	Se connecte via l'instance.

Propriétés du serveur proxy Chiffrement Edge

Le fichier de configuration edgeencryption.properties situé dans le dossier <répertoire d'installation>/conf/ contient des propriétés utilisées pour configurer votre environnement.

Vous devez redémarrer le serveur proxy après avoir apporté des modifications aux propriétés du serveur proxy.

Texte clair et propriétés IV statiques

edgeencryption.customer.assigned.known.cleartext	Effacer le texte pour permettre à l'instance de vérifier que tous les proxys utilisent les mêmes clés. Au démarrage, le proxy chiffre le texte clair et envoie le texte chiffré à l'instance. L'instance ne connaît pas le texte clair et les clés ne sont pas envoyées à l'instance. Cette propriété doit être la même pour tous les proxys.
edgeencryption.encrypter.static.iv	IV statique (vecteur d'initialisation) utilisé dans le chiffrement préservant l'égalité et l'ordre. Cette propriété doit être la même pour tous les proxys et doit être exactement de 16 octets (16 caractères ASCII).

Propriétés de signature numérique

edgeencryption.proxy.signature.keystore.path	Chemin d'accès et nom du fichier Java KeyStore.
edgeencryption.proxy.signature.keystore.password	Mot de passe. Le mot de passe par défaut est <changeme>. Modifiez le mot de passe après l'installation du magasin de clés Java.
edgeencryption.proxy.signature.keystore.keyalias	Alias de clé donné comme argument -alias lors de la génération de la paire de clés RSA.

Propriété de magasin de fichiers

edgeencryption.keyfile.directory	Le répertoire spécifie l'emplacement de stockage des fichiers clés. Si vous utilisez le magasin de clés Java

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	ou un magasin de clés KeySecure SafeNet, laissez cette propriété en commentaire. Exemple : `edgeencryption.keyfile.directory=keys` Si vous utilisez des clés de technologie non liées, ne commentez pas cette propriété et définissez la valeur sur le répertoire des clés.

Propriétés de configuration générales

edgeencryption.config.poll.interval	Intervalle d'interrogation en secondes. Le paramètre par défaut signifie qu'il faut 5 secondes au proxy pour apprendre les changements de configuration de chiffrement. Si les valeurs sont plus élevées, l'instance met plus de temps à détecter un proxy hors ligne. **⚠ Avertissement :** Ne modifiez pas cette propriété. La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lors de la mise en ligne d'un proxy.
edgeencryption.rules.dir	Dossier dans lequel les règles de chiffrement sont stockées sur le proxy.
edgeencryption.encryption.order_preserving.cache.enable	Le paramètre détermine si la mise en cache est utilisée pour prendre en charge les types de chiffrement préservant l'ordre.
edgeencryption.encryption.order_preserving.cache.size	Taille maximale du cache, en octets.
edgeencryption.jobs.concurrency	Nombre maximal de tâches de chiffrement en masse qui peuvent s'exécuter simultanément sur ce proxy.
edgeencryption.jobs.requests_per_second	Nombre de demandes de tâche HTTP par seconde qui peuvent être envoyées à l'instance par ce proxy.
Chiffrement edge.Pièces jointes.Demande.Délai d'expiration.secondes	Délai d'expiration de la demande de chargement de pièce jointe en secondes.
edgeencryption.request.buffer.size	Taille d'une demande de chiffrement. Si une demande de chiffrement est supérieure à cette taille, l'excédent est enregistré sur le disque. **⚠ Avertissement :** Ne modifiez pas cette propriété.
edgeencryption.httpclient.request.buffer.size	Taille de la demande client. Si la demande du client est supérieure à cette taille, l'excédent est enregistré sur le disque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	⚠ Avertissement : Ne modifiez pas cette propriété.
edgeencryption.httpclient.header.size	Taille de l'en-tête de demande/réponse. • Valeur minimale : 8K • Valeur maximale : 32K **⚠ Avertissement :** Ne modifiez pas cette propriété.
edgeencryption.proxy.idle.timeout	Durée en secondes après laquelle une transaction expire. Valeur par défaut : 300 (secondes)
edgeencryption.proxy.keepalive.interval	Durée, en secondes, entre les pings émis par le proxy à l'instance. Des pings sont émis périodiquement pour vérifier la connectivité entre le proxy et l'instance. • Valeur par défaut : 10 (secondes) • Valeur minimale : 5 (secondes)
edgeencryption.register.retry.count	Nombre maximal de fois que le proxy envoie un ping à l'instance pour essayer de l'enregistrer. Valeur par défaut : 0 (aucune limite)
edgecryption.tokenization.exclusion.list	Les modèles de chiffrement ne peuvent pas créer de jetons des chaînes trouvées dans ces champs.

Propriétés du KeyStore Java

edgeencryption.keystore.path	Chemin d'accès au KeyStore Java. Si vous utilisez un magasin de fichiers ou un magasin de clés KeySecure SafeNet, laissez cette propriété en commentaire. Exemple : `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Mot de passe que le proxy utilise pour se connecter au KeyStore Java. Si vous utilisez un magasin de fichiers ou un magasin de clés KeySecure SafeNet, laissez cette propriété en commentaire.

Propriétés de journalisation

Les propriétés de journalisation se trouvent dans le fichier lo4gj2.properties qui se trouve dans le répertoire <installation>/conf/ . Ces propriétés ne sont modifiées que pour le dépannage ou sur demande de l'assistance ServiceNow . Pour plus d'informations, consultez Comment augmenter la journalisation de débogage pour le proxy Chiffrement Edge .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés du magasin de clés de l'appareil NAE

edgeencryption.nae.retries	Nombre de nouvelles tentatives à faire.
edgeencryption.nae.enabled	Le paramètre indique si un appareil NAE est disponible.
edgeencryption.nae.server	Nom du serveur NAE.
edgeencryption.nae.port	Port utilisé par le serveur NAE.
edgeencryption.nae.protocol	Protocole utilisé par le serveur NAE.
edgeencryption.nae.keystore.path	Chemin d'accès au magasin de clés sur le serveur NAE.
edgeencryption.nae.keystore.password	Mot de passe du keystore NAE.
edgeencryption.nae.nom d'utilisateur	Nom d'utilisateur à utiliser pour s'authentifier auprès de l'appareil NAE.
edgeencryption.nae.password	Mot de passe à utiliser pour s'authentifier auprès de l'appareil NAE.
edgeencryption.nae.client.certificate	Certificat situé dans le magasin de clés sur le serveur NAE. Définissez cette propriété pour s'authentifier à l'aide d'un certificat au lieu d'un nom d'utilisateur et d'un mot de passe.

Propriété du mot de passe

edgeencryption.encrypter.properties.password	Nom du fichier dans le dossier `conf` qui contient une chaîne utilisée dans un processus sécurisé pour masquer les mots de passe dans le fichier `edgeencryption.properties` . **Remarque :** Nom du fichier dans le dossier `conf` qui contient une chaîne utilisée dans un processus sécurisé pour masquer les mots de passe dans le fichier `edgeencryption.properties` .

Propriétés de proxy

edgeencryption.proxy.host	Nom de serveur, adresse IP ou nom de domaine complet de l'ordinateur exécutant le proxy. Avec le port, cette propriété définit l'URL utilisée par le client pour accéder au serveur proxy.
edgeencryption.proxy.name	Nom du proxy. Doit être unique pour chaque proxy.
edgeencryption.proxy.http.port	Port sur le proxy pour la communication HTTP.
edgeencryption.proxy.https.port	Port sur le proxy pour la communication HTTPS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété verrouillée de la configuration du proxy

edgeEncryption.proxy.Locked	Si la valeur est vrai, le proxy n'accepte pas les changements de configuration de chiffrement ou les changements de règles de chiffrement à partir de l'instance. Définissez cette propriété sur l'instance de production une fois que toutes les configurations et règles de chiffrement sont définitives.

Propriétés de la base de données du proxy

edgeencryption.db.url	Emplacement de la base de données proxy. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance.
edgeencryption.db.utilisateur	Nom d'utilisateur permettant d'accéder à la base de données proxy. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance.
edgeencryption.db.mot de passe	Mot de passe permettant d'accéder à la base de données proxy. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance.
edgeencryption.db.name	Nom de la base de données proxy. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance. La valeur par défaut de cette propriété est `edgeencryption`.
edgeencryption.db.fichier d'amorce	Fichier d'amorce pour la base de données proxy. Le fichier est relatif au répertoire `sql/` . Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance. **⚠ Avertissement :** Dans des circonstances normales, ne modifiez pas ce paramètre.

Propriétés des performances des serveurs proxy

Par défaut, les propriétés des performances du serveur proxy ne sont pas présentes dans le fichier de configuration. Pour modifier les valeurs par défaut, vous devez ajouter les propriétés et redémarrer le serveur proxy. Pour plus d'informations, consultez Diagnostics et performances de Chiffrement Edge.

edgeencryption.stat.collection.enabled	Active la collecte des statistiques utilisées par le tableau de bord des performances du Chiffrement Edge serveur proxy. Valeur par défaut : true Ajoutez cette propriété et définissez la valeur sur faux pour désactiver la collecte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	de statistiques utilisée par le Chiffrement Edge tableau de bord des performances du serveur proxy.
edgeencryption.stat.collection.interval	Intervalle en secondes pendant lequel le Chiffrement Edge serveur proxy collecte des statistiques. La valeur ne peut pas être inférieure à 30 secondes. Valeur par défaut : 30 (secondes)

Propriétés des certificats SSL

Redémarrez votre proxy si vous modifiez la valeur d'une propriété de certificat SSL. Le système utilise la paire de clés HTTPS au démarrage pour établir la connexion au serveur proxy et déterminer comment le proxy répond aux demandes des clients.

edgeencryption.proxy.https.cert.alias	Alias du certificat fourni par le serveur proxy aux clients de connexion.
edgeencryption.proxy.https.keystore.path	Chemin d'accès au magasin de clés qui contient le certificat HTTPS.
edgeencryption.proxy.https.keystore.password	Mot de passe du magasin de clés qui contient le certificat HTTPS.

Propriétés cibles (instance)

edgeencryption.target.host	Nom d'hôte de l'instance. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l'installation du proxy. Par exemple, instancename.servicenow.com
edgeencryption.target.port	Port d'instance. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l'installation du proxy.
edgeencryption.target.protocol	Protocole d'instance. Doit être le même pour tous les proxys de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l'installation du proxy. Les options incluent : • http • https

Propriétés du fournisseur de technologie non liée

edgeencryption.ekm.provider.classname	Nom de classe interne pour l'implémentation. **⚠ Avertissement :** Ne modifiez pas cette propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

edgeencryption.thirdparty.vendor.library.path	Chemin d’accès au fichier JAR d’API non lié sur l’ordinateur client Unbound.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Alias de clé d’encapsulation dans l’implémentation de la technologie Unbound. Doit être le même pour tous les proxys.

Propriétés du compte utilisateur

edgeencryption.target.username	Nom d’utilisateur que le proxy utilise pour se connecter à l’instance. L’utilisateur doit disposer du rôle edge_encryption. Voir Configurer un compte d’utilisateur Chiffrement Edge.
edgeencryption.target.password	Mot de passe que le proxy utilise pour se connecter à l’instance.

Propriétés du proxy Web

edgeencryption.webproxy.host	Nom du proxy web ou adresse IP.
edgeencryption.webproxy.port	Port sur le proxy web.
edgeencryption.webproxy.user	Nom d’utilisateur utilisé pour se connecter au proxy web. Si votre proxy web n’utilise pas d’authentification, laissez cette propriété en commentaire.
edgeencryption.webproxy.password	Mot de passe à utiliser pour se connecter au proxy web. Si votre proxy web n’utilise pas d’authentification, laissez cette propriété en commentaire.

Propriétés de chiffrement de proxy déconseillées

edgeencryption.encrypter.default.key128

Spécifie le nom de la clé AES 128 actuelle. Une clé AES 128 doit être disponible même si elle n’est pas utilisée. Doit être le même pour tous les proxys.

Effectuez la maintenance de ces clés sur l’instance.

edgeencryption.encrypter.default.key256

Spécifie le nom de la clé AES 256 actuelle. Doit être le même pour tous les proxys.

Effectuez la maintenance de ces clés sur l’instance.

edgeencryption.encrypter.key

Spécifie le nom de clé pour chaque clé et est utilisé pour spécifier les clés par défaut. Il s’agit de l’alias clé intégré aux métadonnées qui est inclus avec chaque élément chiffré et qui est donc stocké sur l’instance. Le nom de la clé doit utiliser des lettres minuscules.

edgeencryption.encrypter.type

Spécifie le type de système de magasin de clés de chiffrement.

edgeencryption.encrypter.file

Spécifie le chemin d’accès et le nom de fichier du fichier texte associé à la clé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

edgeencryption.encrypter.password

Spécifie le mot de passe d'accès au magasin de clés.

Intégration de CyberArk au serveur proxy Edge

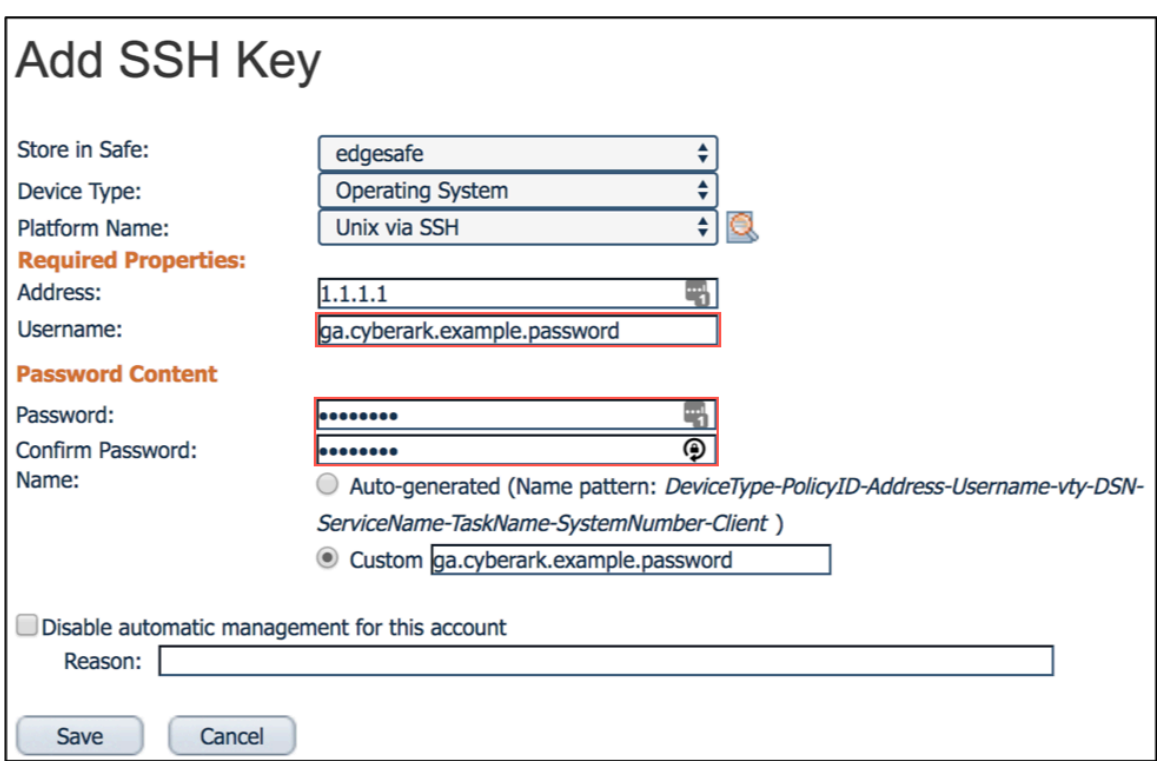
Utilisez CyberArk pour stocker les mots de passe dans un coffre-fort numérique centralisé et sécurisé afin de sécuriser les mots de passe qui étaient auparavant stockés en texte clair et sécurisés par l'accès aux fichiers, ou qui étaient auparavant chiffrés via un deuxième fichier.

CyberArk AIM (Application Identity Management) empêche les accès non autorisés en éliminant les mots de passe codés en dur et visibles. AIM stocke les mots de passe dans un coffre-fort numérique sur un serveur renforcé indépendant, où les mots de passe sont représentés comme des informations d'identification numériques. Les clients AIM (les serveurs proxy Edge) utilisent les identifiants numériques de CyberArk et accèdent au serveur indépendant pour récupérer les mots de passe sécurisés. Aucun mot de passe n'est stocké sur les serveurs proxy Edge ou dans l'instance.

Informations d'identification du coffre-fort numérique CyberArk

Vous devez acheter et configurer CyberArk avant de pouvoir configurer l'intégration de CyberArk avec le serveur proxy Edge.

Pour ajouter des informations d'identification à CyberArk (qui sont lues par le proxy Edge), définissez le **nom de la plateforme** des informations d'identification sur **Unix via SSH** et **assurez-vous** de créer un **nom** d'informations d'identification **personnalisé** ou de noter le **nom** d'informations d'identification généré automatiquement. Lorsque vous configurez le proxy Edge pour utiliser ces informations d'identification, le serveur proxy fait correspondre ce **nom** d'informations d'identification au paramètre du proxy.



Chaque entrée d'identifiant contient un **mot de passe** sécurisé, ainsi qu'un **nom** d'identifiant utilisé par une application pour accéder à ce mot de passe.

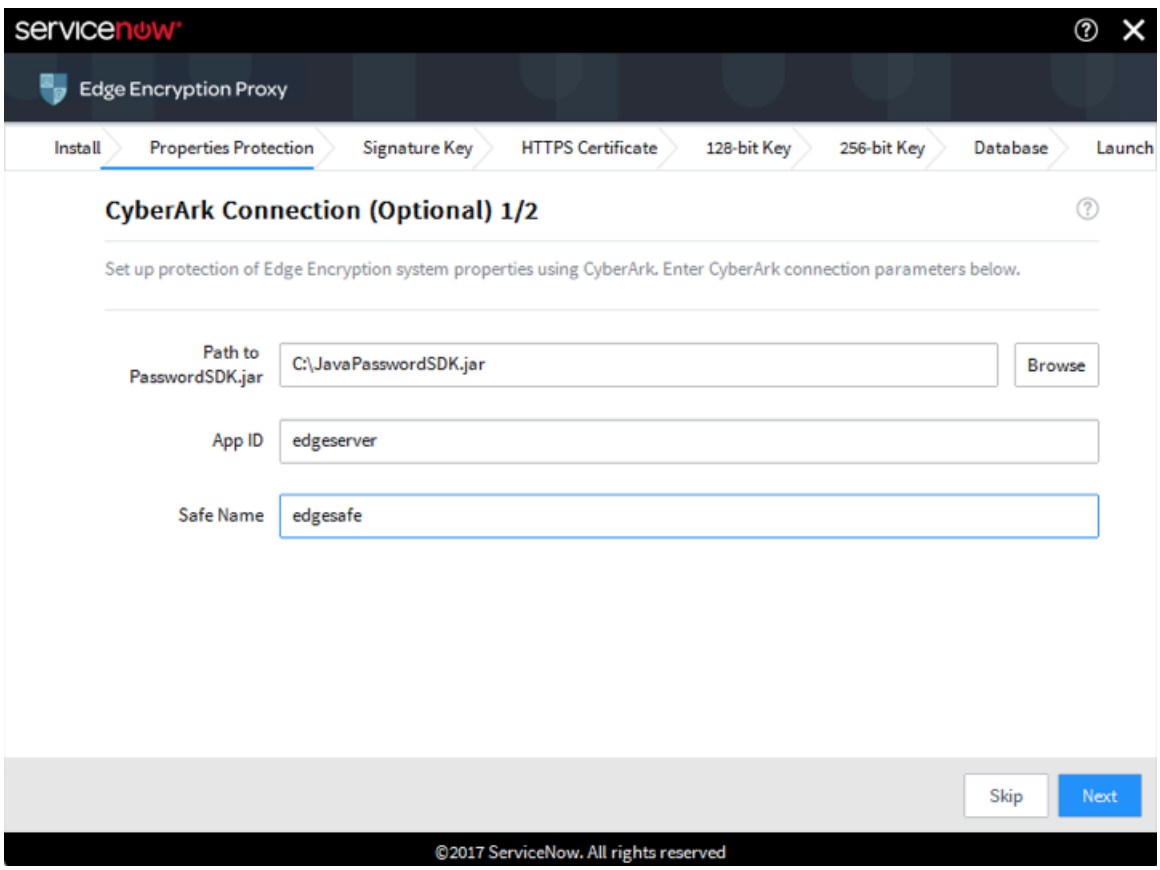
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les informations d'identification CyberArk ne sont pas des clés de chiffrement.

Ajout de CyberArk lors de l'installation d'un proxy Edge

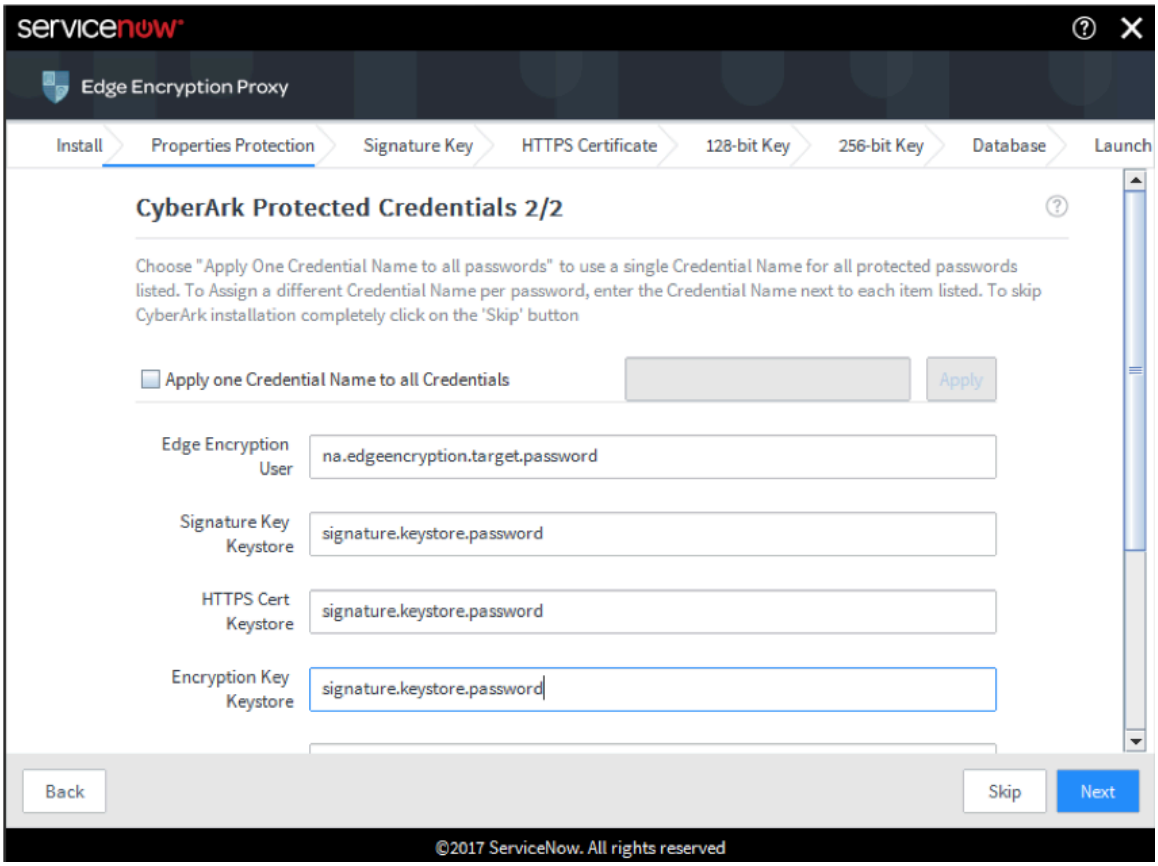
Le programme d'installation du proxy comprend une nouvelle page de configuration pour une intégration CyberArk. Cette page est facultative si vous ne souhaitez pas inclure CyberArk lors de l'installation de votre proxy avec le programme d'installation du proxy. Vous pouvez également installer et configurer manuellement l'intégration de CyberArk dans le fichier de configuration.



Le programme d'installation du proxy comprend également une nouvelle page pour les informations d'identification protégées par CyberArk. Cette page autorise les configurations de différentes propriétés à l'aide d'un ou de plusieurs noms d'informations d'identification. Cette page est facultative si vous ne souhaitez pas inclure CyberArk lors de l'installation de votre proxy avec le programme d'installation du proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Protection par mot de passe de CyberArk

Tout champ de mot de passe du programme d'installation du proxy Edge qui possède des informations d'identification CyberArk configurées dans le coffre-fort de CyberArk et spécifiées sur la page Informations d'identification protégées de CyberArk du programme d'installation est grisé et contient le message Protégé par CyberArk.

Utilisation d'un équilibreur de charge avec le serveur proxy Edge

Vous pouvez utiliser un équilibreur de charge pour équilibrer la charge entre les serveurs proxy de votre configuration de proxy Chiffrement Edge. Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, spécifiez le nom d'hôte et le port HTTPS de l'équilibreur de charge pour permettre aux utilisateurs d'afficher les réponses sur leur navigateur.

Important :
Tous les environnements de production doivent inclure au moins deux serveurs proxy Chiffrement Edge pour la redondance.

Traitement des demandes en périphérie sans équilibreur de charge

Si vous n'utilisez pas d'équilibreur de charge, une demande est traitée comme décrit ci-dessous.

1. L'utilisateur émet une demande à partir d'un navigateur.
2. Le navigateur envoie la demande au serveur proxy Edge.
3. Le serveur proxy envoie la demande à l'instance ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. L'instance ServiceNow renvoie la réponse au serveur proxy.
5. Le serveur proxy ajoute son propre numéro de port dans l'en-tête de la réponse avant de renvoyer la réponse au navigateur de l'utilisateur.

La demande est terminée avec succès, car l'utilisateur peut afficher la réponse du serveur proxy au numéro de port spécifié dans l'en-tête de réponse.

Traitement des demandes en périphérie avec un équilibreur de charge

Toutefois, si vous utilisez un équilibreur de charge, le navigateur de l'utilisateur communique directement avec l'équilibreur de charge, et non avec le serveur proxy. Une demande est traitée comme décrit ci-dessous.

Remarque :
L'exemple suivant utilise 1025 comme numéro de port de serveur proxy.

1. L'utilisateur émet une demande à partir d'un navigateur.
2. Le navigateur envoie la demande à une adresse IP virtuelle d'équilibreur de charge (VIP), également appelée serveur virtuel.
3. L'adresse VIP est configurée pour pointer vers le serveur proxy (par exemple, 10.2.200.148:1025), de sorte que l'équilibreur de charge transmet la demande au serveur proxy.
4. Le serveur proxy envoie la demande à l'instance ServiceNow.
5. L'instance ServiceNow renvoie la réponse au serveur proxy.
6. Le serveur proxy réécrit l'en-tête d'emplacement dans la réponse avec les valeurs configurées dans les propriétés de risk-servicenow.dev.echonet :1025.
   - **Hôte** : edgencryption.proxy.host
   - **Port HTTP** : edgeencryption.proxy.http.port
   - **Port HTTPS** : edgeencryption.proxy.https.port
7. Le serveur proxy transmet la réponse à l'équilibreur de charge avec l'en-tête d'emplacement pointant vers le port du serveur proxy.

Le résultat varie selon que l'équilibreur de charge et les serveurs proxy utilisent le même port.

- Si l'équilibreur de charge et les serveurs proxy utilisent le même port, la demande aboutit, car l'utilisateur reçoit la réponse du même port identifié dans l'en-tête de réponse.
- Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, la demande échoue, car le navigateur de l'utilisateur ne communique qu'avec l'équilibreur de charge, mais la réponse se trouve sur le serveur proxy.

Solution

Vous pouvez résoudre le problème en utilisant simplement l'équilibreur de charge et tous les serveurs proxy Edge sur le même port, mais ce n'est pas une solution idéale. Une meilleure solution consiste à permettre au système de savoir quel port l'équilibreur de charge utilise.

Les propriétés suivantes permettent au serveur proxy Edge de rediriger les messages de réponse vers l'équilibreur de charge si le serveur proxy et l'équilibreur de charge utilisent des ports différents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *edgeencryption.proxy.rewrite.location.host* Spécifie le nom d'hôte utilisé pour accéder à ServiceNow via l'équilibreur de charge.
- *edgeencryption.proxy.rewrite.location.https.port* Spécifie le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge.

Configurer l'équilibreur de charge

Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, spécifiez le nom d'hôte et le port HTTPS de l'équilibreur de charge pour permettre aux utilisateurs d'afficher les réponses sur leur navigateur.

Avant de commencer

Rôles requis :

- administrateur local ou de domaine sur un hôte Windows
- utilisateur de service avec accès complet au système de fichiers sur un hôte Linux

Procédure

1. Connectez-vous à l'hôte du serveur proxy en tant qu'administrateur, administrateur de domaine ou utilisateur de service.
2. Accédez au répertoire d'installation du proxy Edge et sélectionnez conf/edgeencryption.properties.
3. Définissez les propriétés suivantes :

Propriété	Description
edgeencryption.proxy.rewrite.location.host	Si votre configuration Edge inclut un équilibreur de charge pour équilibrer la charge entre les serveurs proxy, réécrit les réponses à l'équilibreur de charge afin que les demandes puissent être effectuées. ○ Si un équilibreur de charge existe dans la configuration du proxy, spécifiez le nom d'hôte utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : Si la configuration du proxy ne contient pas d'équilibreur de charge, vous pouvez définir cette valeur sur le nom d'hôte utilisé par le serveur proxy.
edgeencryption.proxy.rewrite.location.https.port	Si votre configuration Edge inclut un équilibreur de charge pour équilibrer la charge entre les serveurs proxy, spécifie le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Si un équilibreur de charge existe dans la configuration, spécifiez le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : Si la configuration ne contient pas d'équilibreur de charge, vous pouvez définir cette valeur sur le port HTTPS utilisé par le serveur proxy.

4. Enregistrez le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Les demandes peuvent être complétées, car les utilisateurs peuvent désormais afficher les réponses sur leur navigateur.

Mise à niveau de Chiffrement Edge

Les mises à niveau d'instance et les mises à niveau de serveur proxy nécessitent une attention particulière dans un Chiffrement Edge environnement.

Mises à niveau d'instance

Les mises à niveau d'instance dans un environnement Chiffrement Edge nécessitent de la prudence pour s'assurer que les contrôles Edge fonctionnent correctement après la mise à niveau de l'instance.

Lors d'une mise à niveau d'instance, vous ne devez pas ajouter, modifier ou supprimer les éléments suivants :

- Configurations de Chiffrement Edge
- Règles de Chiffrement Edge
- Schémas de création de jetons de Chiffrement Edge
- Travaux planifiés de Chiffrement Edge
- Configurations des clés de chiffrement Edge
- Mises à niveau planifiées de Chiffrement Edge
- Configurations des adresses IP de la liste de refus Chiffrement Edge

Les tâches planifiées en cours d'exécution pendant la mise à niveau de l'instance ne seront pas terminées. Pour terminer la tâche interrompue, réexécutez la tâche une fois que l'instance est mise à niveau. Lorsque vous replanifiez la tâche, le traitement qui s'est produit avant la mise à niveau de l'instance n'est pas perdu et la tâche continue de traiter uniquement les données qui n'ont pas encore été traitées.

Mises à niveau du serveur proxy

Planifiez une mise à niveau du proxy pour permettre à l'instance de mettre à niveau le Chiffrement Edge serveur proxy ou mettez à niveau manuellement le serveur proxy à tout moment.

⚠ Avertissement :
Pour une mise à niveau sous Windows, vous pouvez rencontrer des problèmes de verrouillage des fichiers et la mise à niveau peut échouer. Pour que la mise à niveau réussisse, vous ne devez pas avoir de fichiers ouverts dans le répertoire d'installation. De plus, il ne doit pas y avoir d'interpréteur de commandes existant dans le répertoire d'installation. En particulier, si vous démarrez le proxy à partir de la ligne de commande (via `bin\edgeencryption.bat install/start`) alors que vous êtes dans le répertoire d'installation, vous devez fermer ce shell ou le déplacer hors du répertoire d'installation par la suite. Aucun fichier du répertoire d'installation ne doit être ouvert par un éditeur ou par toute autre application.

Bibliothèques tierces

Les bibliothèques tierces, telles que Gemalto, sont perdues lors des mises à niveau d'instance et de serveur proxy si elles sont conservées dans le même répertoire. Vous pouvez effectuer les opérations suivantes pour éviter la perte de bibliothèques tierces lors des mises à niveau :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Ajoutez manuellement la propriété suivante à edgeencryption.properties :

   `edgeencryption.ekm.provider.classname = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider`

2. Ajoutez la propriété d'emplacement de bibliothèque du *`edgeencryption.thirdparty.vendor.library.path`* fournisseur et définissez-la sur `/path/to/jars`.

   Par exemple :

   `edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs`

3. Copiez les fichiers jar SafeNet dans ce chemin.

Une fois que vous avez installé les bibliothèques tierces en dehors de l'installation Chiffrement Edge , elles ne sont plus perdues lors des mises à niveau.

Mises à niveau planifiées

Important :
Lors ServiceNow des mises à niveau d'instance, mettez également à niveau la version de votre serveur proxy pour l'aligner sur votre version d'instance et réduire les risques de problèmes de compatibilité.

Planifiez une mise à niveau pour permettre à l'instance de mettre à niveau le serveur proxy à l'heure planifiée. Cette fonctionnalité est disponible par défaut après la mise à niveau. Une mise à niveau planifiée inclut les événements suivants :

1. Le serveur proxy vérifie auprès de l'instance s'il existe une nouvelle version disponible pour la mise à niveau. Les nouvelles versions deviennent généralement disponibles lorsque l'instance est mise à niveau.
2. L'administrateur reçoit une notification lors de la connexion lorsqu'une nouvelle version du serveur proxy est disponible.
3. L'administrateur peut planifier une mise à niveau du serveur proxy Chiffrement Edge pour chaque serveur proxy.

   Remarque :
   Seuls les utilisateurs disposant du rôle security_admin peuvent créer un calendrier de mise à niveau via le serveur proxy.

4. Une fois la mise à niveau planifiée, le serveur proxy se met automatiquement à niveau à l'heure planifiée. Pendant la mise à niveau, le serveur proxy n'est hors ligne que pendant une courte période.

   Remarque :
   Étant donné que le serveur proxy redémarre pendant la mise à niveau, il est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

5. Pendant la mise à niveau planifiée, un nouveau répertoire proxy est créé et vos fichiers de configuration sont copiés dans le nouveau répertoire. Les nouvelles propriétés sont écrites dans votre fichier de propriétés existant. Les fichiers ou répertoires suivants dans votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.
   - /conf
   - Répertoire /keys

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- /keystore directory
- fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, vos magasins de clés, vos paramètres et vos certificats sont préservés.

Remarque :
Seuls les fichiers ci-dessus sont copiés dans le nouveau répertoire proxy. Les autres fichiers personnalisés dans le répertoire du serveur proxy ne sont pas conservés lors d'une mise à niveau planifiée. Le fichier journal de mise à niveau se trouve dans le répertoire proxy d'origine dans le dossier suivant : <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Prérequis pour la mise à niveau planifiée

Avant de planifier une mise à niveau pour un proxy Chiffrement Edge, vérifiez ce qui suit :

1. La variable *d'environnement* `JAVA_HOME` pointe vers une installation Java sur l'ordinateur qui se trouve en dehors de la structure de répertoire du proxy Chiffrement Edge.
2. La variable *d'environnement* `JAVA_HOME` pointe vers une installation Java qui se trouve à la version 1.8_u144 ou supérieure.
3. Le `-Djava.io.tmpdir` paramètre du fichier wrapper.conf du proxy Chiffrement Edge pointe vers un répertoire qui est EN DEHORS de la structure de répertoire du proxy Chiffrement Edge, et le proxy a des autorisations de lecture/d'écriture/d'exécution sur le répertoire. En option, vous pouvez commenter entièrement le paramètre afin que Java utilise son emplacement tmp par défaut.

Mises à niveau manuelles

Au lieu de créer un calendrier de mise à niveau, vous pouvez mettre à niveau manuellement chaque serveur proxy via la ligne de commande. Voir Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Linux ou Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Windows.

État de la version du proxy

Vous pouvez facilement déterminer si un serveur proxy est obsolète en accédant à **Configuration de Chiffrement Edge** > **Proxys** > **Tous**. L'état de la version de votre proxy est indiqué dans la colonne **Version du proxy** par les couleurs suivantes :

Vert

Votre serveur proxy est à jour.

Jaune

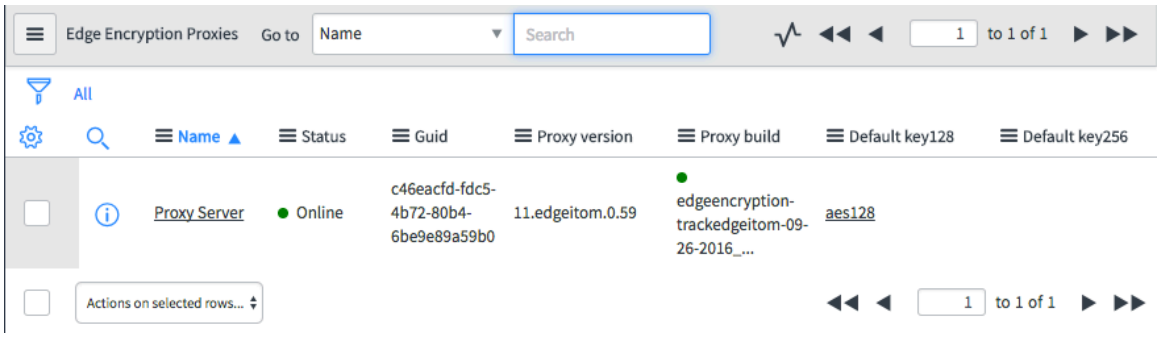
Votre serveur proxy est obsolète et une mise à niveau est nécessaire.

Orange

Nous n'avons pas pu procéder à la mise à niveau. Votre serveur proxy revient à l'ancienne version pour s'assurer qu'il n'y a pas de temps d'arrêt.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Résoudre un problème d'échec de mise à niveau de proxy planifiée

Lorsqu'une mise à niveau de proxy planifiée échoue, le serveur proxy revient à la version à partir de laquelle vous effectuez la mise à niveau. Toutes les données, clés et fichiers de configuration d'origine sont conservés. Ce processus peut prendre plusieurs minutes. Contacter Service client et assistance pour s'assurer que la mise à niveau a réussi.

Pour déterminer le motif de la défaillance, vous pouvez vérifier le motif de la **défaillance** dans le calendrier de mise à niveau. En outre, le répertoire d'installation de la mise à niveau ayant échoué est conservé afin que les fichiers journaux soient disponibles pour le dépannage.

Remarque :
Avant de supprimer des répertoires proxy supplémentaires, vérifiez toujours quel répertoire est en cours en examinant les fichiers journaux. Si les fichiers journaux ont une activité récente, le proxy est peut-être connecté à votre instance.

Si une mise à niveau de proxy programmée échoue à plusieurs reprises, vous pouvez mettre à niveau manuellement votre serveur proxy. Consultez Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Linux et Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Windows.

Configuration minimale requise pour Java

La machine hôte installant ou exécutant le Chiffrement Edge serveur proxy doit maintenir une version prise en charge de Java. Les versions prises en charge actuelles sont Java 17.0.3 ou version ultérieure dans la série de versions 17.x.

Remarque :
Java 11 n'est plus pris en charge à partir de la version Yokohama. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 17 avant d'essayer d'installer Yokohama ou des versions ultérieures Chiffrement Edge du proxy.

Si vous utilisez le chiffrement AES 256 bits avec Java 8 update 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte du serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de règles de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Environnements mixtes de versions proxy

Bien qu'il ne soit pas recommandé d'utiliser un environnement exécutant d'anciennes versions du serveur proxy avec des versions à jour du serveur proxy, il est pris en charge si tous les serveurs proxy appartiennent à la même famille de versions que votre instance. Par

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

exemple, si vous avez une instance sur la Yokohama version, votre environnement prend en charge les serveurs proxy à partir de n'importe quel Yokohama correctif ou correctif chaud. Toutefois, les limitations suivantes s'appliquent.

- Si un serveur proxy prend en charge des fonctionnalités qu'un autre proxy ne prend pas en charge, vous constaterez un comportement incohérent, selon le serveur proxy utilisé.
- Si un serveur proxy est obsolète, il peut ne pas inclure les améliorations de sécurité récentes.

Si un serveur proxy d'une version précédente est enregistré avec une version plus récente de l'instance, vous recevrez régulièrement des notifications indiquant que le serveur proxy est obsolète. Pour garantir un environnement optimal et sécurisé, ServiceNow recommande de toujours mettre à niveau votre serveur proxy vers la version la plus récente du logiciel pris en charge par votre instance.

Planifier une mise à niveau du serveur proxy Chiffrement Edge

Créez un calendrier de mise à niveau pour permettre à l'instance de mettre à niveau un serveur proxy obsolète.

Avant de commencer

Pour planifier une mise à niveau, vous devez être connecté à votre instance via le serveur proxy.
Si vous utilisez le chiffrement AES 256 bits avec Java 8 update 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte du serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de règles de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Une fois la mise à niveau planifiée, le serveur proxy se met automatiquement à niveau à l'heure planifiée. Pendant la mise à niveau, le serveur proxy n'est hors ligne que pendant une courte période.

Remarque :
Étant donné que le serveur proxy redémarre pendant la mise à niveau, il est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

Pendant la mise à niveau planifiée, un nouveau répertoire proxy est créé et vos fichiers de configuration sont copiés dans le nouveau répertoire. Les nouvelles propriétés sont écrites dans votre fichier de propriétés existant. Les fichiers ou répertoires suivants dans votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.

- /conf
- Répertoire /keys
- /keystore directory
- fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, vos magasins de clés, vos paramètres et vos certificats sont préservés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Seuls les fichiers ci-dessus sont copiés dans le nouveau répertoire proxy. Les autres fichiers personnalisés dans le répertoire du serveur proxy ne seront pas conservés lors d'une mise à niveau planifiée. Le fichier journal de mise à niveau se trouve dans le répertoire proxy d'origine dans le dossier suivant : <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Si plusieurs serveurs proxy sont obsolètes, vous devez planifier une mise à niveau pour chaque serveur proxy individuellement.

Remarque :
Évitez d'héberger plusieurs serveurs proxy sur la même machine. Toutefois, si votre environnement inclut cette configuration, ne planifiez pas de mises à niveau vers plusieurs proxys sur le même ordinateur en même temps.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Proxys** > **Calendriers de mise à niveau**.
2. Cliquez sur **Nouveau**.
3. Complétez le formulaire.

Formulaire Calendrier de mise à niveau du proxy Chiffrement Edge

Champ	Description
Serveur proxy	Serveur proxy en cours de mise à niveau.
Version cible	Version vers laquelle vous mettez à niveau votre serveur proxy. Cette valeur est en lecture seule et définie sur la version de proxy la plus à jour disponible pour votre instance.
Heure de début planifiée	Date et heure de début de la mise à niveau.
Actifs	Indique si la mise à niveau planifiée est active. Si ce champ n'est pas sélectionné, la mise à niveau ne sera pas effectuée aux date et heure planifiées.
États	L'état de la mise à niveau. Cette valeur est en lecture seule. Les états possibles sont les suivants : ○ En attente ○ En cours d'exécution ○ Terminé ○ Échoué

4. Cliquez sur **Envoyer**.

Que faire ensuite

La durée typique d'une mise à niveau est inférieure à 15 minutes. Une fois qu'une mise à niveau est exécutée, vous pouvez examiner les détails de la mise à niveau pour en savoir plus. En cas d'échec de votre mise à niveau, consultez la raison de la **défaillance** pour déterminer les étapes suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de mise à niveau

Champ	Description
À partir de la version	Version à partir de laquelle le serveur a été mis à niveau.
Vers la version	Version vers laquelle le serveur a été mis à niveau.
Heure de début réel	Heure à laquelle la mise à niveau a commencé.
Heure de fin	Heure à laquelle la mise à niveau s'est terminée.
Cause de la défaillance	Motif de l'échec de la mise à niveau.

Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Linux

Mettre à jour un proxy exécuté sous Linux.

Avant de commencer

Si vous utilisez le chiffrement AES 256 bits avec Java 8 update 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte du serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de règles de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : administrateur security_admin ou local sur l'ordinateur hôte

Procédure

1. Téléchargez le fichier d'archive Chiffrement Edge proxy-update dans le répertoire d'installation.
   a. Accédez à la **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**
   b. Sélectionnez le lien **Télécharger le programme d'installation de ligne de commande** .
   c. Lorsque le téléchargement commence, sélectionnez votre répertoire d'installation comme emplacement de téléchargement.
2. Accédez au répertoire d'installation.
3. Exécutez la commande suivante :

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade -c <répertoire proxy>
```

Option	Description
Répertoire proxy	Répertoire du répertoire d'installation où le proxy a été installé initialement. Ce répertoire est créé par l'installation.

Si vous souhaitez afficher l'écran d'aide, exécutez cette commande sans arguments : `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Un nouveau répertoire proxy est créé avec un horodatage actuel. Une sauvegarde de l'ancien répertoire proxy est conservée en tant que backup.dist-upgrade_timestamp dans le nouveau répertoire d'installation du proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’ancien proxy s’arrête et le nouveau proxy démarre. Toutes les connexions/transactions ouvertes sur l’ancien serveur proxy sont terminées.

4. Vérifiez le journal du proxy dans le nouveau répertoire et l’instance pour vérifier que le nouveau proxy est en cours d’exécution.

Mettre à niveau manuellement un serveur proxy Chiffrement Edge exécuté sous Windows

Mettre à jour un proxy exécuté sous Windows.

Avant de commencer

Si vous utilisez le chiffrement AES 256 bits avec Java 8 update 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte du serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d’effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de règles de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : administrateur security_admin ou local sur l’ordinateur hôte

Procédure

1. Téléchargez le fichier d’archive Chiffrement Edge proxy-update dans le répertoire d’installation.
   a. Accédez à la **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**
   b. Sélectionnez le lien **Télécharger le programme d’installation de ligne de commande** .
   c. Lorsque le téléchargement commence, sélectionnez votre répertoire d’installation comme emplacement de téléchargement.
2. Démarrez le programme de terminal cmd Windows avec des privilèges d’administrateur.
3. Accédez au répertoire d’installation.
4. Exécutez la commande suivante :

```
Java -jar edgeencryption-dist-<version>-all.jar -m dist-upgrade -c <répertoire proxy>
```

Option	Description
Répertoire proxy	Répertoire du répertoire d’installation où le proxy a été installé initialement. Ce répertoire est créé par l’installation.

Si vous souhaitez afficher l’écran d’aide, exécutez cette commande sans arguments : `java -jar edgeencryption-dist-<version>-all.jar`

Un nouveau répertoire proxy est créé avec un horodatage actuel. Une sauvegarde de l’ancien répertoire proxy est conservée en tant que backup.dist-upgrade_timestamp dans le nouveau répertoire d’installation du proxy. L’ancien proxy s’arrête et le nouveau proxy démarre. Toutes les connexions/transactions ouvertes sur l’ancien serveur proxy sont terminées.

5. Vérifiez le journal du proxy dans le nouveau répertoire et l’instance pour vérifier que le proxy a été mis à jour et est en cours d’exécution.

Restaurer une mise à niveau du serveur proxy Chiffrement Edge

Si une mise à niveau du proxy échoue, vous pouvez revenir à la version antérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Si une mise à niveau échoue lors de l'utilisation de la fonctionnalité de mise à niveau planifiée dans la Yokohama version, le serveur proxy restaure automatiquement l'ancienne version. L'ancien serveur proxy est stocké sans modification dans un répertoire de sauvegarde.

Si vous souhaitez restaurer une mise à niveau manuelle, vous pouvez procéder comme suit.

Procédure

1. Fermez le proxy.
2. Supprimez le nouveau répertoire proxy.
3. Renommez le répertoire de sauvegarde avec le nom du proxy.
   Le répertoire de sauvegarde se trouve dans le répertoire d'installation du proxy avec le nom <nom du proxy>_backup
4. Démarrez le proxy.
5. Vérifiez le journal du proxy et l'instance pour vérifier que le proxy est en ligne.

Configuration de Chiffrement Edge

Une fois le serveur proxy installé et en cours d'exécution Chiffrement Edge , effectuez la gestion Chiffrement Edge via le serveur proxy.

Vous devez effectuer toutes les étapes avant Installation de Chiffrement Edge de créer des configurations de chiffrement et des modèles de chiffrement sur l'instance.

Remarque :
Pour accéder à la Chiffrement Edge configuration, vous devez vous connecter via le serveur proxy et accéder au rôle security_admin.

Rotation des clés de chiffrement

Effectuez la rotation de la clé de chiffrement à partir de l'instance. Ajoutez une nouvelle clé, modifiez l'affectation de clé par défaut, puis planifiez une rotation de clés en masse ou une rotation de clés unique.

Avant de définir une clé de chiffrement comme clé par défaut, rendez la clé disponible pour chaque proxy. Cela garantit que les proxys disposent de la clé pour chiffrer les données lorsque la clé est affectée comme clé par défaut. Tous les proxys doivent avoir accès à une clé avant que cette clé puisse être affectée comme clé par défaut.

Avertissement :
Avant de supprimer une clé du proxy, configurez et exécutez une tâche de rotation de clés en masse pour vous assurer qu'aucune donnée de l'instance n'utilise la clé. Si des informations sont toujours chiffrées avec cette clé, vous ne pouvez pas les déchiffrer après avoir supprimé la clé.

Comportement de filtrage et de tri des bordures

Chaque fois que vous modifiez les clés par défaut, assurez-vous d'effectuer une rotation de clés (soit en masse, soit en rotation de clés unique). Dans le cas contraire, vous risquez de recevoir des résultats inattendus lors du tri et du filtrage des enregistrements. Imaginons par exemple le scénario suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Vous créez des enregistrements chiffrés à l'aide d'une clé de chiffrement.
2. Vous créez une nouvelle clé et la définissez par défaut.
3. Vous créez un ensemble d'enregistrements chiffrés à l'aide de la nouvelle clé de chiffrement.

Si vous filtrez par un champ chiffré lorsque vous êtes connecté via le proxy Edge, tous les enregistrements peuvent ne pas être filtrés correctement ou des enregistrements peuvent apparaître de manière inattendue. Le filtre fonctionne uniquement pour les enregistrements chiffrés à l'aide de la clé par défaut actuelle. Les enregistrements chiffrés à l'aide de la clé par défaut précédente apparaissent toujours dans la vue de liste.

Si vous triez par un champ chiffré lorsque vous êtes connecté via le proxy Edge, vous voyez deux groupes d'enregistrements avec le même texte lisible par l'homme dans le champ chiffré.

Planifier une seule tâche de rotation de clé

Planifiez une tâche pour rechercher des données chiffrées à l'aide d'un alias de clé spécifié, puis chiffrez à nouveau les données avec la clé de chiffrement par défaut actuelle. Les données sont déchiffrées avant d'être à nouveau chiffrées avec la clé par défaut.

Avant de commencer

Rôle requis : security_admin

Avant de planifier cette tâche, mettez à jour la clé par défaut dans **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Définir les clés par défaut**.

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation de clé unique**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	**Sélectionnez Rotation de clé unique**.
Clé	Entrez la clé à mettre hors service. Vérifier que cette clé n'est plus la clé par défaut dans **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Définir les clés par défaut**.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Non disponible lors de l'exécution d'une seule rotation de clés.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ de la table Audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Ce champ est en lecture seule et actif. Pour en savoir plus sur les champs audités, consultez Audit.
Estimer le nombre	Nombre maximal estimé d'enregistrements audités à traiter. Non disponible lors de l'exécution d'une seule rotation de clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
d'enregistrements d'audit maximal	
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
Estimer le nombre d'enregistrements n'est pas pris en charge lors du traitement des champs audités.

Planifier une tâche de rotation des clés en masse

Planifiez une tâche pour rechercher des données chiffrées avec une clé précédente, puis chiffrez à nouveau les données avec les clés de chiffrement par défaut actuelles. Les données sont déchiffrées avant d'être à nouveau chiffrées avec la clé par défaut actuelle.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation de clés en masse**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Rotation de clés en masse**.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Non disponible lors de l'exécution d'une rotation de clés en masse.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ de la table Audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Ce champ est en lecture seule et actif. Pour en savoir plus sur les champs audités, consultez Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Non disponible lors de l'exécution d'une rotation de clés en masse.
Actifs	Décochez cette case pour désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   Estimer le nombre d'enregistrements n'est pas pris en charge lors du traitement des champs audités.

Planifier une tâche de rotation clé de pièce jointe

Planifiez une tâche pour rechercher des pièces jointes chiffrées à l'aide d'un alias de clé spécifié, puis chiffrez de nouveau les pièces jointes avec la clé de chiffrement par défaut actuelle. La pièce jointe est déchiffrée avant d'être chiffrée à nouveau avec la clé par défaut.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation clé des pièces jointes**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **la rotation clé de la pièce jointe**.
Actifs	Décochez la case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Nombre d'enregistrements estimé.**
5. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Chiffrer les champs à l'aide de configurations de chiffrement

Chiffrez les champs en créant des configurations de chiffrement.

Pour configurer Chiffrement Edge, vous devez être connecté à l'instance via le proxy. Testez tous les changements sur une instance de non-production avant de les appliquer à l'instance de production.

Définir les clés de chiffrement

Après avoir configuré un ou plusieurs proxys et une clé de chiffrement par défaut, l'instance vérifie que les clés sont disponibles pour tous les proxys. Vous ne pouvez pas faire d'une clé de chiffrement la clé par défaut à moins que tous les proxys n'aient la clé. Une fois qu'une clé par défaut est définie, vous pouvez créer des configurations de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecter les champs et les pièces jointes à chiffrer

L'affectation de champs et de pièces jointes à chiffrer implique l'affectation d'un type de chiffrement au champ ou à la pièce jointe. Avant de marquer un champ comme chiffré, évaluez ces problèmes.

- Déterminez les fonctionnalités système susceptibles d'être impactées.
- Examinez tous les scripts pour vérifier l'utilisation du champ.
- Apportez les ajustements souhaités à la taille du champ. Une fois qu'un champ a été configuré pour le chiffrement, la taille du champ ne peut pas être modifiée.

Le marquage d'un champ à chiffrer agrandit la taille du champ pour stocker les données chiffrées. Le processus d'extension de la taille du champ peut prendre beaucoup de temps, en fonction du nombre d'enregistrements dans la table.

Prise en charge de l'API

Chiffrement de champ met à jour les API `setDisplayValue()` et `setValue()` afin qu'elles puissent insérer des données chiffrées pour les champs chiffrés. Il permet également à `getDisplayValue()` et `getValue()` de renvoyer des valeurs en texte clair.

Le script suivant illustre ces changements d'API lorsque la brève description de l'incident est chiffrée :

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Lorsque vous utilisez `getValue()` pour obtenir du texte chiffré, votre script ne renvoie plus le texte chiffré. Votre script renvoie le texte en clair, en supposant que l'utilisateur a accès au module de chiffrement. `getValue()` renvoie le texte chiffré si l'utilisateur n'a pas accès au module cryptographique.

Créer une configuration de chiffrement de champ

Sélectionnez les champs à chiffrer et identifiez le type de chiffrement.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Créer**.
2. Renseignez le formulaire.

Champ	Description
Table	La table qui contient le champ à chiffrer.
Type	Indique s'il faut chiffrer une colonne de table ou des pièces jointes pour la table. **Sélectionnez une colonne**.
Colonne	Champ à chiffrer. S'affiche uniquement lorsque le **type** est **Colonne**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Seuls les champs Chaîne, Date, Date/Heure, Journal, Entrée de journal et URL sont pris en charge. ○ **Champs de chaîne et d'URL** : vous pouvez ajouter une configuration de chiffrement à une table parente ou à une table enfant. ○ **Champs Date et Date/Heure** : vous ne pouvez ajouter une configuration de chiffrement qu'à une table parente. Vous ne pouvez pas ajouter une nouvelle configuration de chiffrement à une table enfant. **Remarque :** Selon le nombre d'enregistrements affectés par les champs Date et Date/Heure que vous chiffrez, la création de la configuration de chiffrement peut prendre jusqu'à quelques minutes. Assurez-vous de créer la configuration de chiffrement pour les champs Date et Date/Heure lorsque le volume de transactions sur l'instance est faible.
Type de chiffrement	Le type de chiffrement à utiliser.

Remarque :
Une combinaison de table et de champ spécifique ne peut avoir qu'une seule configuration active à la fois.

3. Cliquez sur **Envoyer**.

Que faire ensuite
Après avoir ajouté l'enregistrement de configuration de chiffrement, vous pouvez créer une tâche de chiffrement pour chiffrer les données existantes. Si vous n'exécutez pas de tâche de chiffrement, Edge chiffre les données existantes la prochaine fois que les données changent. Pour plus de détails, voir Planifier une tâche de chiffrement.

Créer une configuration de chiffrement variable

Sélectionnez les variables de catalogue de services à chiffrer et identifiez le type de chiffrement.

Avant de commencer
Rôle requis : security_admin

Procédure
1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable**.
2. Dans la liste **Configurations des variables de chiffrement Edge** , cliquez sur **Nouveau**.
3. Renseignez le formulaire.

Champ	Description
Variable	La variable à chiffrer.
Type de chiffrement	Le type de chiffrement à utiliser.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Après avoir ajouté l'enregistrement de configuration de chiffrement, vous pouvez créer une tâche de chiffrement pour chiffrer les données existantes. Si vous n'exécutez pas de tâche de chiffrement, Edge chiffre les données existantes la prochaine fois que les données changent. Pour plus de détails, voir Planifier une tâche de chiffrement.

Désactiver une configuration de chiffrement

Après avoir configuré le chiffrement d'un champ ou des pièces jointes d'une table, vous pouvez arrêter le chiffrement en désactivant la configuration du chiffrement. Après avoir désactivé le chiffrement, vous pouvez exécuter une tâche de déchiffrement pour les champs ou une tâche de déchiffrement de pièce jointe pour les pièces jointes afin de supprimer les données chiffrées de l'instance.

Avant de commencer

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

⚠ Avertissement :
La désactivation d'une configuration de chiffrement ne supprime pas l'enregistrement de chiffrement et le type de chiffrement ne peut pas être modifié.

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de Chiffrement Edge** > **Tous**.
   La liste **des configurations de Chiffrement Edge** s'affiche.
2. Cliquez sur la configuration de chiffrement à désactiver.
   Le formulaire **Configuration de Chiffrement Edge** s'affiche.
3. Cliquez sur la case **Actif** .
   La zone **Actif** est dégagée.
4. Cliquez sur **Mettre à jour**.
   La liste **des configurations de Chiffrement Edge** s'affiche.

Que faire ensuite

Vous pouvez exécuter une tâche de déchiffrement ou de déchiffrement de pièce jointe pour déchiffrer les données sur l'instance. Si vous n'exécutez pas de tâche, les données chiffrées sont déchiffrées la prochaine fois qu'elles sont modifiées.

Planifier une tâche de chiffrement

Vous pouvez planifier une tâche pour rechercher et chiffrer toutes les données non chiffrées dans un champ spécifié, à l'aide de la clé de chiffrement par défaut configurée pour le champ. Si vous ne créez pas de tâche de chiffrement après avoir configuré un champ pour le chiffrement, seules les nouvelles valeurs sont chiffrées.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous** pour créer une tâche pour un champ ou **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable** pour créer une tâche pour une variable.
2. Cliquez sur le champ pour lequel vous souhaitez planifier une tâche de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sous **Liens connexes**, cliquez sur **Planifier la tâche de chiffrement en masse**.

   Le formulaire **Tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. Le bas du formulaire affiche les enregistrements de toutes les exécutions de tâches précédentes.

4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Type de travail	Sélectionnez **Chiffrement**.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Rempli après avoir sélectionné **Estimer le nombre d'enregistrements**.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ de la table Audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Pour en savoir plus sur les champs audités, reportez-vous à la section Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Rempli après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque l'option **Enregistrements d'historique du processus** est sélectionnée. **Remarque :** L'estimation peut être supérieure au nombre réel d'enregistrements traités.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Planifier une tâche de déchiffrement

Vous pouvez planifier une tâche pour déchiffrer des données dans un champ chiffré, afin de stocker des données claires dans l'instance.

Avant de commencer

Remarque :
Vous devez marquer l'enregistrement de chiffrement du champ comme inactif (décochez la case **Actif**) pour exécuter la tâche de déchiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous** pour créer une tâche pour un champ ou **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable** pour créer une tâche pour une variable.
2. Cliquez sur le champ que vous souhaitez déchiffrer.
3. Sous **Liens connexes**, cliquez sur **Planifier la tâche de déchiffrement en masse**.

   Le formulaire **Tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. Le bas du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Déchiffrement**.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Rempli après avoir sélectionné **Estimer le nombre d'enregistrements**.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ de la table Audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Pour en savoir plus sur les champs audités, reportez-vous à la section Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Rempli après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque l'option **Enregistrements d'historique du processus** est sélectionnée. **Remarque :** L'estimation peut être supérieure au nombre réel d'enregistrements traités.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Chiffrer les pièces jointes à l'aide du chiffrement standard

Vous pouvez chiffrer les pièces jointes pour des tables spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutes les pièces jointes à une table utilisent le même type de chiffrement. Les pièces jointes chiffrées ne sont pas recherchées lors d'une recherche de texte. Seuls les types de chiffrement standard sont autorisés pour les pièces jointes. Les types de chiffrement préservant l'ordre ou l'égalité ne sont pas autorisés.

Pour une session en contournant le Chiffrement Edge proxy :

- Sur un enregistrement dont le chiffrement de la pièce jointe est activé :
  - L'utilisateur peut voir qu'il y a des pièces jointes et les noms des pièces jointes.
  - L'utilisateur ne peut pas ajouter de nouvelles pièces jointes.
- Sur un enregistrement sans chiffrement de pièce jointe activé :
  - L'utilisateur peut ouvrir et télécharger des pièces jointes existantes.
  - L'utilisateur peut ajouter de nouvelles pièces jointes.

Pour une session à l'aide du proxy de chiffrement, l'utilisateur peut ouvrir et télécharger des pièces jointes existantes et ajouter de nouvelles pièces jointes.

Configurer le chiffrement de la pièce jointe

Sélectionnez les tables dont les pièces jointes doivent être chiffrées et identifiez le type de chiffrement.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Configurations de Chiffrement Edge** > **Créer**.
2. Renseignez les champs du formulaire comme il convient.

Configuration de Chiffrement Edge

Champ	Description
Table	Sélectionnez une table dont les pièces jointes doivent être chiffrées.
Type	Indique s'il faut chiffrer une colonne de table ou des pièces jointes pour la table. Sélectionnez **Pièce jointe**.
Colonne	Champ de table à chiffrer. Ce champ s'affiche lorsque le **type** est **Colonne** et non lorsque le **type** est **Pièce jointe**.
Type de chiffrement	Le type de chiffrement à utiliser. Pour les pièces jointes, seuls AES128 standard et AES256 standard sont autorisés.

3. Cliquez sur **Envoyer**.

Que faire ensuite

Une fois l'enregistrement de chiffrement ajouté, vous pouvez créer une tâche de chiffrement de pièce jointe pour chiffrer les pièces jointes existantes. Si vous n'exécutez pas de tâche de chiffrement de pièce jointe, le système chiffre les nouvelles pièces jointes lorsque vous les joignez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous marquez `l'attribut edge_encryption_clear_attachment_allowed` comme **True** dans l'entrée Dictionnaire de collecte de la table, les pièces jointes non chiffrées sont ajoutées à une table à l'aide de Chiffrement Edge pour chiffrer les pièces jointes. Si cet attribut est activé, vous devez configurer une tâche de chiffrement des pièces jointes afin que toutes les pièces jointes non chiffrées ajoutées soient chiffrées.

Planifier une tâche de chiffrement de pièce jointe

Vous pouvez planifier une tâche pour rechercher et chiffrer toutes les pièces jointes non chiffrées pour une table spécifiée, à l'aide de la clé de chiffrement par défaut configurée pour la table.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous**.
2. Cliquez sur la table pour laquelle vous souhaitez planifier une tâche de chiffrement.
3. Sous **Liens connexes**, cliquez sur **Planifier la tâche de chiffrement en masse**.

   Le formulaire **Tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. Le bas du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Type de travail	Sélectionnez **Chiffrement de la pièce jointe**.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Planifier une tâche de déchiffrement de pièce jointe

Vous pouvez planifier une tâche pour déchiffrer toutes les pièces jointes chiffrées pour une table spécifiée, afin de stocker les pièces jointes effacées dans l'instance.

Avant de commencer

Remarque :
Vous devez marquer l'enregistrement de chiffrement de la table comme inactif (décochez la case **Actif**) avant que la tâche de déchiffrement ne s'exécute, sinon rien ne se passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous**.
2. Cliquez sur la table contenant les pièces jointes que vous souhaitez déchiffrer.
3. Sous **Liens connexes**, cliquez sur **Planifier la tâche de déchiffrement en masse des pièces jointes**.

   Le formulaire **Tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. Le bas du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Déchiffrement de la pièce jointe**.
Actifs	Décochez la case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Modifier le type de chiffrement d'un champ ou d'une pièce jointe

Vous pouvez modifier le type de chiffrement d'un champ ou d'une pièce jointe en sélectionnant un nouveau type de chiffrement dans l'enregistrement de configuration de chiffrement existant. Une combinaison de table et de champ spécifique ne peut avoir qu'une seule configuration active à la fois.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous**.
   La liste **des configurations de Chiffrement Edge** s'affiche.
2. Ouvrez l'enregistrement pour que la configuration de chiffrement soit modifiée.
3. Cliquez sur la liste déroulante **Type de chiffrement** et sélectionnez un nouveau type de chiffrement.

Remarque :
Pour les pièces jointes, seuls AES128 standard et AES256 standard sont autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Si nécessaire, exécutez une tâche de chiffrement ou de chiffrement de pièce jointe .
   Il n'est pas nécessaire d'exécuter une tâche de chiffrement. Si vous n'exécutez pas de tâche de chiffrement, le champ ou la pièce jointe est chiffré à l'aide du nouveau type de chiffrement lors de la prochaine modification du champ ou de la pièce jointe.

Segmenter les chaînes à l'aide de schémas de chiffrement

Vous pouvez remplacer les modèles de chaîne par des jetons avant qu'ils ne soient envoyés et stockés dans l'instance.

Avant de commencer

Pour utiliser des modèles de chiffrement, vous devez installer et configurer une base de données MySQL dans votre réseau. Il s'agit de la même base de données utilisée pour le chiffrement préservant l'ordre. Pour créer ou modifier des modèles de chiffrement, vous devez être connecté à l'instance via le proxy.

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des modèles de système de base ou créer vos propres modèles. Les modèles de système de base sont des modèles avancés. Les modèles de chiffrement incluent les limitations suivantes.

- Un modèle de tous les caractères alpha n'est pas autorisé.
- La taille minimale du modèle est de cinq caractères. Vous pouvez modifier ce paramètre à l'aide d'une propriété système.
- Les quantificateurs * et + sont interdits dans les modèles de chiffrement.
- Les modèles de chiffrement correspondent à des mots complets, et non à des parties de chaînes intégrées dans une chaîne plus grande. Les mots sont définis par des espaces et des caractères qui ne peuvent pas être inclus dans un modèle.
- Si la même chaîne est envoyée plusieurs fois à l'instance, elle est remplacée par le même jeton.
- La recherche de texte sur les correspondances exactes est prise en charge. La chaîne de requête est échangée avec un jeton lorsqu'elle est envoyée à l'instance, la recherche est effectuée sur les jetons et lorsque les résultats de la recherche sont renvoyés au serveur proxy, les jetons sont remplacés par le texte clair. Les fonctionnalités telles que la création de racines ne sont pas prises en charge.

Lorsque vous utilisez des modèles, le texte clair ne quitte jamais votre réseau. Lorsque le serveur proxy correspond à un modèle dans une requête destinée à l'instance, le proxy remplace la chaîne par un jeton de même taille. Le jeton est envoyé à l'instance au lieu de la chaîne de texte clair. Lorsque la réponse est envoyée de l'instance au serveur proxy, le proxy remplace le jeton par la chaîne. Lorsqu'elle est affichée via le serveur proxy, la chaîne s'affiche sous forme de texte clair.

Remarque :
Les champs chiffrés ne sont pas vérifiés pour les modèles de chiffrement.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Schémas de chiffrement** > **Créer**.
   Vous pouvez également accéder aux **modèles avancés** pour activer ou modifier un modèle préconfiguré.
2. Saisissez le nom du modèle.
3. Définissez le **type d'entrée du modèle de bordure**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Élémentaire	Une série de types de caractères. Dans l'onglet **En trée de modèle de base** , cliquez sur **Ajouter** et sélectionnez un type de caractère. **L'exemple de modèle** affiche le modèle au fur et à mesure que des caractères sont ajoutés. Cliquez sur **Nouveau bloc** pour déplacer le caractère suivant à la ligne suivante. Cela vous permet de regrouper des caractères dans un modèle long. Cliquez sur **X** pour supprimer le dernier ca–ractère du modèle.
Avancé	Expression RegEx Java. Si l'option Avancé est sélectionnée, vous ne pouvez pas revenir au type d'entrée de base. Dans le champ **Exemple de correspon dance** , entrez un exemple de modèle pour tester l'expression RegEx. Dans le champ **Modèle** , entrez une expression RegEx Ja–va. Cliquez sur **Valider** pour vérifier que l'expression correspond à l'exemple de modèle.

Le type d'entrée définit la façon dont vous allez entrer le modèle. Elle n'a pas d'impact sur la façon dont le modèle est utilisé.

4. Cliquez sur **Envoyer**.

Réparer ou récupérer les données chiffrées préservant l'ordre

Si vous disposez du rôle security-admin, vous pouvez planifier des tâches effectuées par le proxy pour réparer ou récupérer les champs qui utilisent le chiffrement de préservation de l'ordre Chiffrement Edge .

Planifiez les tâches pour :

- Jetons d'ordre de réparation.
- Recréez la base de données proxy.

L'exécution de ces tâches peut être une opération longue qui peut avoir un impact sur les Chiffrement Edge performances du proxy. Planifiez ces tâches à un moment où aucun utilisateur ou un ensemble minimal d'utilisateurs n'utilisent le système, par exemple minuit le week-end.

Planifier une tâche de réparation de jeton de commande

Vous pouvez planifier une tâche pour rechercher et réparer les champs dans lesquels le jeton de commande est manquant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche
Utilisez ces tâches pour réparer des champs individuels dans une table ou pour réparer tous les champs à l'aide du chiffrement préservant l'ordre. Exécutez cette tâche lorsque la base de données proxy a été hors ligne pendant l'exécution de l'instance, ce qui permet de préserver l'ordre des champs pour lesquels des jetons d'ordre sont manquants.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la réparation des jetons de commande**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Réparation de jeton de commande**.
Tous les champs	Cochez cette case pour réparer toutes les tables.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de la tâche pour la première fois.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Nombre d'enregistrements estimé.**

Planifier une tâche de récupération de base de données proxy

Exécutez cette tâche lorsque la base de données proxy a perdu des données. Cette tâche trouve tous les enregistrements qui ont été chiffrés avec un jeton (type de chiffrement préservant l'ordre) et les envoie au proxy afin que la base de données du proxy puisse être reconstruite.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la récupération de la base de données**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Entrez un nom descriptif pour cette tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Type de travail	Sélectionnez **Récupération de base de données**.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure d'exécution de cette tâche pour la première fois.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.

Configurer la liste de refus d'adresse IP

Empêcher une adresse IP de votre réseau d'envoyer des requêtes à votre instance

Avant de commencer

Rôle requis : security_admin

Étant donné que le Chiffrement Edge serveur proxy réside dans votre réseau, il peut être soumis à des analyses de vulnérabilité par votre logiciel réseau. Pour empêcher le transfert d'un scanner IP ou d'autres demandes à votre ServiceNow instance, vous pouvez ajouter des adresses IP, des plages IP ou des masques de réseau à une liste de refus. Toute connexion au serveur proxy à partir d'une adresse refusée est interrompue et n'est pas transférée à votre instance.

Pour placer une adresse IP sur une liste de refus, vous devez être connecté à votre instance via le serveur proxy.

Important :
Assurez-vous de bien comprendre la topologie de votre réseau avant d'ajouter des adresses IP à une liste de refus. Si une adresse IP est ajoutée à la liste de refus, tout utilisateur possédant cette adresse IP ne pourra pas accéder au Chiffrement Edge serveur proxy.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Maintenance** > **Liste de refus des adresses IP**.
   La vue de liste Listes de refus des adresses IP du proxy de chiffrement [edge_encryption_ip_blacklist] s'ouvre.
2. Cliquez sur **Nouveau**.
3. Complétez le formulaire.

Champ	Description
Serveur proxy	Serveur Chiffrement Edge proxy qui est empêché de transférer les demandes des adresses figurant sur la liste de refus.
Adresse IP, plage d'adresses IP ou masque réseau	Les demandes provenant de cette adresse IP, de cette plage ou de ce masque de réseau ne sont pas transmises à votre ServiceNow instance. Voici quelques exemples de valeurs : ○ Adresse IP : 10.10.10.5 ○ Plage IP : 10.10.10.1-15 ○ Masque réseau : 10.10.10.0/24

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous pouvez utiliser des adresses IPv4 ou IPv6
Actif	Indique si l'enregistrement est actif ou non. Seules les adresses IP des enregistrements actifs sont empêchées d'envoyer des demandes à l'instance.
Description	Description de l'enregistrement de la liste de refus.

4. Cliquez sur **Envoyer**.
5. Répétez ces étapes pour tous les autres proxys pour lesquels une adresse IP doit être refusée.

Résultats

Le Chiffrement Edge serveur proxy met fin à toute connexion à partir d'adresses IP, de plages ou de masques de réseau figurant sur la liste de refus et ne peut pas transmettre la demande à l'instance.

Chiffrer les données d'un créateur d'enregistrement

Configurez votre Chiffrement Edge serveur proxy pour autoriser les insertions à partir d'un créateur d'enregistrement en créant des règles de chiffrement à partir de l'enregistrement du créateur d'enregistrement.

Avant de commencer

Rôle requis : security_admin

Les créateurs d'enregistrements permettent aux utilisateurs finaux de créer des enregistrements basés sur des tâches, tels que des enregistrements d'incidents, à partir du Catalogue de services et Portail de services. Si un créateur d'enregistrement tente d'insérer des données dans un champ marqué pour chiffrement, un message d'insertion non valide s'affiche et les données ne sont pas enregistrées dans le champ.

Le chiffrement des données d'un créateur d'enregistrement nécessite une configuration de chiffrement définie pour le champ cible. Vérifiez que vous avez créé une configuration de chiffrement pour le champ et la table cibles avant de créer une règle de chiffrement à partir d'un créateur d'enregistrement. Voir Créer une configuration de chiffrement de champ. Pour chiffrer les pièces jointes d'un créateur d'enregistrement, Configurer le chiffrement de la pièce jointe.

Procédure

1. Connectez-vous à votre instance via le Chiffrement Edge serveur proxy.
2. Accédez à la **Catalogue de services** > **Définitions de catalogues** > **Créateurs d'enregistrements**.
3. Créez un enregistrement de créateur d'enregistrement ou ouvrez un enregistrement de créateur d'enregistrement existant.
4. Sous **Liens connexes**, sélectionnez **Créer une règle Chiffrement Edge**.
   Deux règles de chiffrement inactives sont automatiquement créées pour chiffrer les données envoyées par le créateur d'enregistrement au champ marqué pour chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle de chiffrement	Description
<RecordProducerName>	Règle créée pour traiter les Catalogue de services paramètres POST des variables de mappage et des champs de l'instance.
<RecordProducerName>Json	Règle créée pour traiter une charge utile JSON à partir de et Portail de services mapper les variables aux champs de l'instance.

5. Activez les règles de chiffrement nécessaires créées par le créateur d'enregistrement.

   a. Accédez à la **Configuration de Chiffrement Edge** > **Règles** > **Tous**.

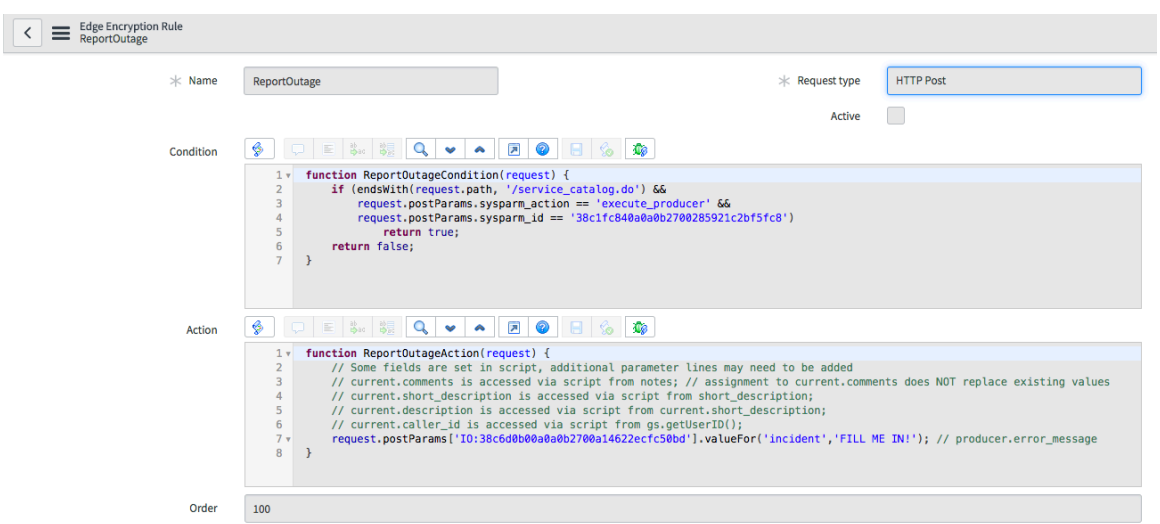
   b. Selon l'endroit où le créateur d'enregistrement sera utilisé, ouvrez la règle de chiffrement associée créée par le créateur d'enregistrement et sélectionnez le marqueur **Actif** .
   Si vous utilisez le créateur d'enregistrement dans le Catalogue de services, activez la règle de chiffrement <RecordProducerName>. Si vous utilisez le créateur d'enregistrement dans le Portail de services, activez la règle de chiffrement <RecordProducerName>Json.

6. **Facultatif :** Examinez le champ Action de la règle **de** chiffrement et ajoutez les noms de champs ou instructions nécessaires.

   (Optional) Si un créateur d'enregistrement mappe directement une variable à un champ d'une table, la règle de chiffrement mappe automatiquement la variable au champ approprié. Toutefois, si une variable est indirectement mappée par le biais de différents scripts sur la plateforme, vous devrez peut-être mettre à jour les règles pour mapper chaque variable au champ approprié.

   Example

   (Optional) La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement Signaler une panne et traite les paramètres POST à Catalogue de services partir du pour mapper les variables aux champs de l'instance. Remplacez « REMPLIR MOI » par le champ cible.

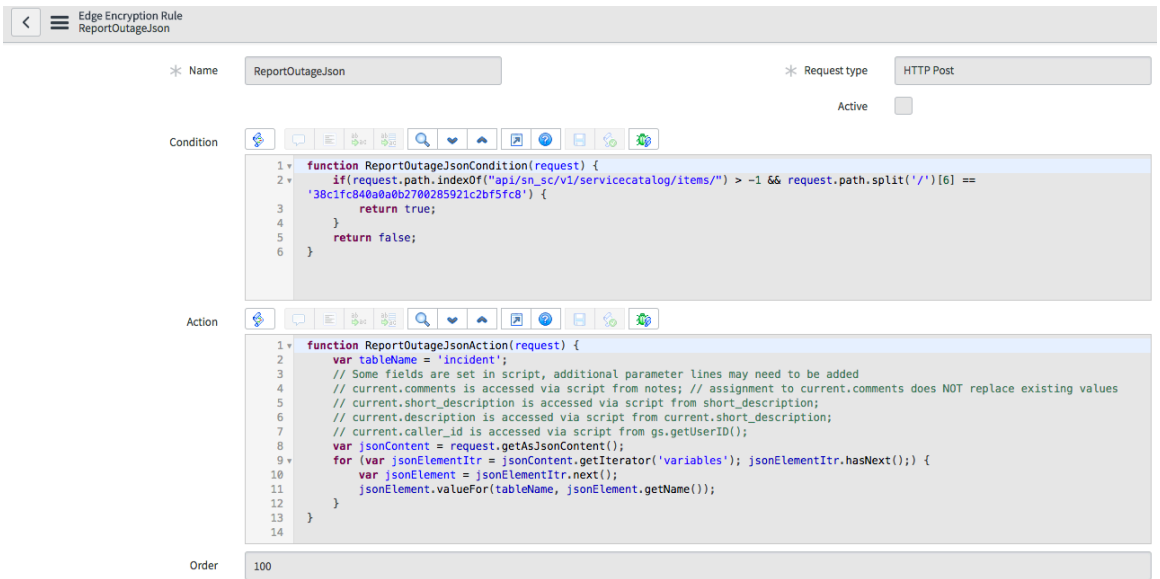


   La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement de rapport de panne et traite une charge utile JSON à partir de pour Portail de services mapper

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les variables aux champs de l'instance. Ajoutez des instructions supplémentaires pour mapper toutes les variables scriptées aux champs cibles.



Lorsque la charge utile du créateur d'enregistrement est examinée, l'élément error_message contient la valeur du champ short_description. En ajoutant l'instruction suivante, vous pouvez mapper la variable scriptée error_message au champ short_description.

```
if (jsonElement.getName() == 'error_message')
      jsonElement.valueFor(tableName, 'short_description');
```

La valeur du champ **Action** devient :

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need to be added
 // current.comments is accessed via script from notes; // assignment to current.comments
 does NOT replace existing values
 // current.short_description is accessed via script from short_description;
 // current.description is accessed via script from current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
            } else {
        jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Résultats

Les deux règles de chiffrement permettent au créateur d'enregistrement d'insérer des valeurs dans les champs marqués pour chiffrement à partir du ou Portail de services.Catalogue de services

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir une règle de chiffrement personnalisée

Il peut être nécessaire d'identifier et de chiffrer les informations sensibles dans les requêtes HTTP sur le chemin de votre instance. Vous pouvez écrire des règles de chiffrement pour identifier, interpréter et chiffrer les données de ces demandes, en mappant les champs de la demande aux noms de champs de table sur votre instance.

Qu'est-ce qu'une règle de chiffrement ?

Les règles de chiffrement sont des scripts exécutés sur le Chiffrement Edge serveur proxy pour mapper les champs d'une demande aux champs d'une table de votre ServiceNow instance. Une règle de chiffrement indique au serveur proxy comment chiffrer les Chiffrement Edge données dans des charges utiles personnalisées.

Remarque :
Les règles de chiffrement ne prennent en charge que ECMAScript 3 et les versions antérieures.

Quand utiliser des règles personnalisées

Un ensemble de règles de chiffrement est inclus dans le module d'extension Chiffrement Edge . Ces règles gèrent de nombreux cas d'utilisation de la plateforme principale, tels que :

- Modifier un champ à partir du formulaire de modification de liste
- Mettre à jour un enregistrement à partir du formulaire d'enregistrement
- Gestion du service Web direct
- Traitement des données à partir de l'interface de programmation d'application (API) REST

Les applications créées à l'aide de formulaires et de listes standard doivent fonctionner sans règles de chiffrement personnalisées.

Si vous développez des scripts qui contiennent des données qui doivent être chiffrées, créez des règles de chiffrement pour trouver et mapper ces données aux noms de champs de table Glide. Par exemple :

- Processeurs de script
- Services Web basés sur un script
- API REST, interfaces utilisateur ou scripts Ajax scriptés

Format d'une règle de chiffrement

Les règles comprennent trois parties :

- **Condition** : identifie le type de demande.
- **Action** : mappe les champs de la demande aux champs d'une table, en chiffrant les valeurs qui correspondent aux champs dont les configurations de chiffrement sont définies.
- **Ordre** : priorité de la règle. La règle de priorité la plus basse avec une condition satisfaite est la seule règle qui s'exécute. Comme les règles métier, les règles s'exécutent de la plus basse à la plus élevée.

À l'exception des demandes de pièces jointes, les demandes HTTP sont évaluées par le Chiffrement Edge serveur proxy. Le Chiffrement Edge serveur proxy évalue toutes les conditions de règle de chiffrement par ordre de priorité jusqu'à ce que toutes les conditions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

retournent la valeur faux, ou qu'une condition renvoie la valeur vrai. Lorsqu'une condition renvoie la valeur vrai, l'action est exécutée sur la demande et le résultat est transmis à l'instance. Aucune autre condition n'est évaluée. Par conséquent, les conditions de la règle de chiffrement doivent être aussi spécifiques que possible. Une règle générique peut être évaluée comme vraie pour une demande destinée à être traitée par une autre règle, ce qui entraîne le traitement de la demande par une action incorrecte. Si une condition générique est inévitable, la règle doit être marquée d'une valeur d'ordre élevé afin que des règles plus spécifiques soient évaluées en premier.

Directives pour la création de règles de chiffrement

La création de règles de chiffrement efficaces et optimisées peut réduire le temps de traitement de la validation des scripts.

Ligne directrice générale : Lorsque les règles deviennent longues, faites de votre mieux pour minimiser le nombre de blocs et briser les règles dans la mesure du possible. Idéalement, les règles personnalisées devraient s'appliquer à des cas d'utilisation spécifiques, plutôt que d'englober plusieurs cas, avec des instructions `if` ou switch dans le script d'action.

1. Séparez les règles dans la mesure du possible. Par exemple :
   - Créez des règles différentes pour différentes tables et assurez-vous que chaque règle s'exécute uniquement sur sa table respective.
   - Créez des règles différentes pour chaque créateur d'enregistrements que vous ciblez, ou au moins pour chaque sous-ensemble de créateurs d'enregistrements. Au lieu d'une règle ciblant des dizaines de `sys_ids`, vous pouvez créer plusieurs règles différentes ciblant de plus petits sous-ensembles de créateurs d'enregistrements, ou même créer une règle par `sys_id`.

     Remarque :
     La création de plusieurs règles nécessite plus de maintenance. Le compromis est que plusieurs règles plus simples peuvent être validées plus efficacement que des règles plus longues et plus complexes.

2. Minimisez le nombre de blocs. Étant donné que le moteur de traitement analyse chaque bloc lors de l'évaluation des scripts, un grand nombre de blocs entraîne des retards de validation. Par exemple :
   - Remplacez tous les blocs `if` par une recherche de tableau, et remplacez tous les blocs de la recherche de tableau par un seul bloc `if` .
   - Combinez `les blocs if` chaque fois qu'il est possible de les regrouper.

API de règles de chiffrement

Les règles de chiffrement sont écrites en JavaScript et utilisent Chiffrement Edge des API pour localiser et chiffrer les informations sensibles dans le corps d'une demande. L'API utilise des expressions similaires à xPath pour naviguer dans le contenu JSON et XML.

Chiffrement Edge Les API traitent la demande hors du flux au fur et à mesure de son écriture dans le flux de sortie. L'analyse de flux permet aux règles de chiffrement d'être performantes sur le réseau. Cependant, l'extraction et l'analyse du contenu du corps plusieurs fois peuvent entraîner des résultats inattendus. Pour annuler ce problème potentiel, les demandes doivent être traitées par l'action en un seul passage.

Lors de la création de règles de chiffrement, vous ne pouvez pas utiliser les API Glide, les includes de script, les règles métier ou tout autre paramètre global tel que `actuel`. Étant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

donné que les règles sont créées pour les objets HTTP, un objet de `demande` globale est disponible.

Lors de la création de règles de chiffrement, vous ne pouvez pas utiliser les API du gestionnaire de liste d'autorisation ou des applications incluses dans le périmètre.

Gestion des erreurs

Si une condition ou une action de règle de chiffrement lève une exception, consultez le journal de proxy pour obtenir des informations de dépannage.

Inspecter la demande du client

Avant de créer une règle de chiffrement personnalisée, vous devez déterminer le format de la demande du client entrant dans le Chiffrement Edge serveur proxy.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Étant donné que les règles de chiffrement itérent sur les demandes des clients et déterminent ce qui doit l'être, le cas échéant, vous devez comprendre le type de demande pour lequel vous créez une règle. Le format de la demande du client détermine la structure de votre règle de chiffrement et les API disponibles pour utilisation dans la règle.

Procédure

1. Inspectez la demande du client.

   Selon la source de la demande, les outils suivants sont disponibles pour inspecter la demande et déterminer le format.

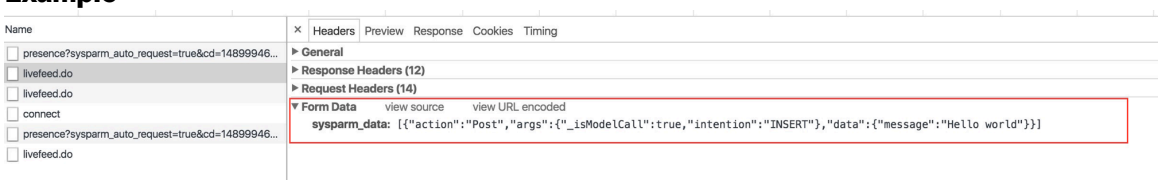
Source de la demande	Outils disponibles
Navigateur du client	Utilisez la console développeur de votre navigateur pour inspecter la demande du client. Les outils utiles incluent : ○ Moniteur réseau Firefox ○ Panneau réseau Chrome
Source tierce/externe	Utilisez un analyseur de protocole HTTP pour inspecter la demande. Les outils utiles incluent : ○ Wireshark ○ HTTP Scoop Sinon, vous pouvez souvent utiliser la documentation de la source externe pour déterminer le format de la demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. À partir de la demande du client, inspectez le paquet et déterminez :
   - Méthode de demande du client
   - Adresse URL de la demande
   - Les paramètres d'URL
   - Paramètres POST, le cas échéant
   - Format du corps de la demande, s'il est inclus

Example



Résultats
L'inspection de la demande permet de comprendre les champs que vous devez filtrer et itérer dans votre règle de chiffrement. Pour comprendre les champs de l'objet *de demande* , reportez-vous à la section Demande.

Créer une règle de chiffrement

Les règles de chiffrement sont utilisées par le proxy pour trouver du contenu dans les requêtes HTTP qui doit être chiffré.

Avant de commencer
Rôle requis : security_admin
Avant de créer une règle de chiffrement, vous devez Inspecter la demande du client déterminer le format.

Pourquoi et quand exécuter cette tâche
Pour créer ou modifier des règles de chiffrement, vous devez être connecté à l'instance via un proxy de chiffrement.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Règles** > **Créer**.
2. Dans la zone **Nom** , entrez un nom.
3. Dans le **Type de demande**, sélectionnez une méthode HTTP.
   - **HTTP Post**
   - **HTTP Get**
   - **Put HTTP**
   - **Correctif HTTP**
   - **HTTP Delete**

   Remarque :
   Les instances préalablesJakarta n'autorisent que **les méthodes HTTP Get** et **HTTP Post** .
4. Dans la zone **Condition** , saisissez une instruction JavaScript définissant quand la règle doit s'exécuter.
5. Dans la zone **Action** , saisissez une fonction JavaScript à exécuter si la condition équivaut à vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la zone **Ordre** , entrez la priorité relative de la règle.
7. Cliquez sur **Soumettre** ou enregistrez le formulaire.

Conditions de règle de chiffrement

Les conditions de la règle de chiffrement déterminent si la règle doit être exécutée.

Une condition de règle de chiffrement doit retourner true si la règle doit gérer la requête HTTP ; sinon, il doit retourner la valeur Faux.

Lorsque vous créez votre condition, gardez à l'esprit qu'une seule règle est exécutée par demande. Par conséquent, la condition doit être aussi générale ou spécifique que nécessaire pour fonctionner dans les circonstances prévues.

Remarque :
Soyez prudent lorsque vous effectuez des vérifications du contenu dans la condition. Des vérifications excessives peuvent être coûteuses pour le serveur proxy et entraîner une latence accrue lors du traitement de requêtes complexes.

La condition peut utiliser le type de méthode, le type de contenu, le chemin d'accès URL ou tout autre paramètre de chaîne de requête URL pour déterminer si la règle doit traiter la demande. La condition a accès à ces champs via l'objet Demande . Avant de créer une condition de règle de chiffrement, assurez-vous d'avoir inspecté la demande du client et de comprendre les conditions nécessaires pour déclencher la règle.

Remarque :
Pour créer des règles efficaces, envisagez des moyens simples d'exclure les demandes que vous ne souhaitez pas voir évaluées par une règle. Configurez votre condition pour qu'elle renvoie d'abord la valeur faux pour ces demandes. Cette méthode augmente les performances et achemine rapidement la demande vers la règle correcte.

Objets de règle de chiffrement et API sont disponibles pour les conditions de règle de chiffrement.

Exemple utilisant path et postParams

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
     return true;
  }
  return false;
}
```

Exemple utilisant urlParams et contentType

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 &&
 request.xmlContains('myXmlTag')) {
     return true;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
  }
 return false;
}
```

Actions de règle de chiffrement

Une règle de chiffrement mappe les champs d'une demande client aux champs d'une table de votre instance et identifie les champs marqués pour chiffrement.

Une action de règle de chiffrement s'exécute uniquement lorsque la condition de la règle de chiffrement renvoie la valeur vrai. Une règle de chiffrement identifie les données à chiffrer dans la charge utile de votre demande. Étant donné que la règle itère le contenu de l'objet de demande, vous devez comprendre la forme et la structure du corps de votre demande et déterminer ce qui doit être chiffré dans la demande. Les données à chiffrer peuvent se trouver dans :

- Un paramètre POST ou URL.
- Contenu JSON ou XML dans un paramètre POST ou URL.
- Une charge utile JSON .
- Une charge utile XML .

Avant d'écrire une action de règle de chiffrement, veillez à :

- Inspecter la demande du client.
- Identifiez l'emplacement des données sensibles dans l'objet de la demande .
- Déterminez le nom du champ et de la table dans lequel insérer des données, ou comprenez comment les extraire dynamiquement de la demande.

Objets de règle de chiffrement et API sont disponibles pour les actions et conditions de règle de chiffrement.

Objets de règle de chiffrement et API

Utilisez les API de règles de chiffrement pour analyser et chiffrer les valeurs des demandes qui transitent par le Chiffrement Edge serveur proxy jusqu'à l'instance.

Les API disponibles pour votre règle de chiffrement dépendent du format de l'objet de demande. Par exemple, si le paramètre contentType de l'objet de demande est XML, vous pouvez utiliser le API XML pour analyser et chiffrer les valeurs dans la charge utile. Une fois que vous avez déterminé le type d'objet dans votre demande, vous pouvez créer une règle de chiffrement à l'aide des API disponibles.

Les API de règles de chiffrement sont disponibles dans les scripts de condition et d'action de règle de chiffrement.

Demande

L'objet `request` est un objet global disponible dans les scripts d'action de règle et de Chiffrement Edge condition.

L'objet `request` est un objet JavaScript qui représente la requête du client arrivant sur le Chiffrement Edge serveur proxy. Vous devez créer votre règle de chiffrement pour analyser l'objet de la *demande* , mapper les valeurs de l'objet de la *demande* aux champs d'une table de l'instance et chiffrer toutes les données sensibles dans l'objet de la *demande* .

L'objet de *demande* comprend les attributs et données suivants de la demande du client :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'objet de demande

Champ	Description
chemin d'accès	La partie chemin d'accès de l'URL.
requestMethod	OBTENIR, PUBLIER, METTRE, CORRIGER, SUPPRIMER.
contentType	Le champ d'en-tête Type de contenu.
urlParams	Les paramètres de la chaîne de requête. Cela peut également être évalué dans une chaîne.
postParams	S'il s'agit d'une publication de formulaire, elle contient les paramètres de publication.

demande : getAsJsonContent()

Renvoie la demande en tant qu'objet itérable de type `JsonNode`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle si le corps de la demande est une charge utile JSON valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de la `demande` .

Une fois la demande renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser le API JSON pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande sous forme de `JsonNode` itérable.

demande : getAsXmlContent()

Renvoie le contenu de la demande sous forme d'objet itérable de type `XMLContent`.

Cette méthode n'est disponible dans une Chiffrement Edge règle que si le corps de la demande est une charge utile XML valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de la `demande` .

Une fois que la demande est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser le API XML pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLContent	La demande en tant qu'objet itérable de type `XMLContent`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

demande : XMLContains(chemin d'accès de la chaîne)

Renvoie la valeur vrai si le chemin d'accès donné existe dans les DOM XML.

Cette méthode n'est disponible que si le corps de la demande est une charge utile XML valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de la *demande* .

Paramètres

Nom	Type	Description
chemin d'accès	Chaîne	Instruction XPath que vous recherchez.

Renvoie

Type	Description
Booléen	Indique si le chemin d'accès donné existe dans les DOM XML.

API des paramètres POST et URL

Les paramètres POST et URL sont accessibles en tant que propriétés *de l'objet* de demande à l'aide de request.postParams et request.urlParams.

N'importe quel paramètre unique est accessible en tant que propriété des objets parents *postParams* et *urlParams* en appelant request.postParams.myParam. Tout paramètre accessible de cette manière est un objet de la classe sous-jacente *ParameterValue*. Toutes les API de cette classe peuvent être appelées sur n'importe quel paramètre.

Après avoir inspecté la demande du client, il peut être nécessaire d'accéder aux valeurs des paramètres et de les chiffrer à partir de l'objet de la *demande* . Selon les données de la demande client, vous pouvez chiffrer les valeurs et les mapper aux champs de l'instance de plusieurs façons.

Chiffrer la valeur d'une table et d'un champ connus

Si vous connaissez le nom de la table d'instance et du champ qui contiendra les données chiffrées, vous pouvez les définir explicitement dans la règle de chiffrement. Par exemple, vous pouvez savoir que la demande sera traitée sur l'instance pour créer un incident et vous souhaitez chiffrer le paramètre de **texte** dans le champ de description. Dans ce cas, vous pouvez créer l'action suivante.

```
function SampleAction1() {
   request.postParams.text.valueFor('incident', 'description');
}
```

Chiffrer la valeur d'une table et d'un champ définis dynamiquement

Si, à l'inverse, vous ne connaissez pas le nom du champ que les données chiffrées rempliront, vous pouvez les définir dynamiquement à l'aide de **tableName** et **fieldName**.

L'exemple ci-dessous traite une demande générique qui peut stocker des données dans différentes tables de tâches (telles que incident, problème et change_request) sur l'instance.

```
function SampleAction2() {
   var tableName = request.urlParams.table;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'text') {
            currentParam.valueFor(tableName, 'description')
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Cette action :

- Obtient la table de destination à partir des paramètres d'URL.
- Itère sur les paramètres d'URL.
- Demande au serveur proxy de chiffrer n'importe quel paramètre d'URL Chiffrement Edge avec un nom qui correspond à un champ marqué pour chiffrement.
- Recherche un paramètre spécifique appelé `texte` et demande au Chiffrement Edge proxy de chiffrer la valeur en fonction de la configuration de chiffrement pour le champ Description sur la table Incident.

Dans cet exemple, la méthode valueFor() n'effectue en fait aucun chiffrement. Au lieu de cela, la méthode demande Chiffrement Edge au serveur proxy de vérifier si la paire table/champ dans l'objet de la demande est marquée pour chiffrement avec une configuration de chiffrement et, le cas échéant, de la chiffrer.

Chiffrer JSON ou XML dans un paramètre

Un paramètre POST ou URL peut inclure du contenu JSON ou XML. Dans ce cas, vous pouvez traiter le contenu dans le paramètre, itérer sur les valeurs et chiffrer les champs requis. Dans cet exemple, le **tableName** est toujours accessible à partir d'un paramètre POST, mais la valeur du champ est les **données** de l'objet JSON.

```
function SampleAction3() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsJsonContent().iterator();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

Exemple d'une action de règle de chiffrement qui traite du code XML dans un paramètre POST.

```
function SampleAction4() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}
```

Chiffrer une requête

Vous pouvez rencontrer une requête codée dans un paramètre de la demande client qui contient des données sensibles. Pour faire correspondre un champ d'une requête à une valeur chiffrée dans la base de données d'instance, vous devez créer une règle de chiffrement qui demande au proxy de vérifier si un champ de la requête est marqué pour le chiffrement. La méthode encodedQueryFor() analyse une requête codée sur une table donnée et vérifie si certains champs de la requête ont des configurations de chiffrement.

Dans cet exemple, la règle itère les paramètres à la recherche du paramètre de **filtre** , qui doit être une requête codée Glide.

```
function SampleAction5() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'filter') {
            currentParam.encodedQueryFor(tableName);
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

Par exemple, si la valeur du **filtre** est : `short_description=Mes informations sensibles^numéro=INC000056^catégorie=Panne`, la requête devient `short_description=<Chiffré(Mes informations sensibles)>^numéro=INC000056^catégorie=Panne` sur l'instance.

ParameterValue : toString()

Convertit la valeur du paramètre POST ou URL en chaîne.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Valeur du paramètre sous forme de chaîne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ParameterValue : getAsJsonContent()

Renvoie la demande en tant qu'objet itérable de type `JsonNode`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle si le corps de la demande est une charge utile JSON valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de la `demande` .

Une fois la demande renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser le API JSON pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande sous forme de `JsonNode` itérable.

ParameterValue : getAsXmlContent()

Renvoie le contenu de la demande sous forme d'objet itérable de type `XMLContent`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle. Cette méthode suppose que le corps de la demande est une charge utile XML valide. Vous pouvez vérifier le contentType pour vous en assurer.

Une fois que la demande est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser le API XML pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLContent	La demande en tant qu'objet itérable de type `XMLContent`.

ParameterValue : encodedQueryFor(String tableName)

Spécifie que la valeur de l'élément est une requête codée sur la table spécifiée.

L'appel de cette fonction sur un paramètre indique au proxy que la valeur du paramètre est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les champs de la requête codée qui doivent être chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous prévoyez que la requête s'exécute.

Renvoie

Type	Description
nul	

ParameterValue : valueFor(String tableName, String fieldName)

Spécifie que la valeur de l'élément est mappée au champ spécifié dans la table spécifiée.

L'appel de cette méthode sur une valeur d'élément indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Renvoie

Type	Description
nul	

API XML

Les API XML peuvent être utilisées après l'appel de `getAsXmlContent()sur l'objet` de demande ou une propriété `ParameterValue` .

Lorsque vous utilisez des API XML pour écrire votre règle de chiffrement, vous pouvez suivre un format général :

1. Appelez `getAsXmlContent()sur l'objet` de demande ou la propriété `ParameterValue` . Cela renvoie un objet itérable de la classe `sous-jacente XMLContent` .
2. Appelez `getIterator()` ou `getIterator(String xPath)` sur l'objet `XMLContent` . Cela renvoie un objet `XMLElementIterator` qui peut être utilisé pour itérer sur des éléments XML.
3. Appelez la méthode `hasNext()` sur l'objet `XMLElementIterator` pour déterminer si un autre élément est disponible.
4. Appelez `next()` sur l'objet `XMLElementIterator` pour renvoyer l'élément XML suivant. Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Appelez `valueFor(String tableName, String fieldName)` sur l'élément XML. Cette méthode indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

Remarque :
Pour déterminer si vous souhaitez appeler `valueFor(String tableName, String fieldName)` sur un élément XML, vous pouvez utiliser la méthode `getName()` pour renvoyer le nom de l'élément.

Mappage à un champ de table connu sur l'instance

Dans cet exemple, la charge utile XML sera traitée sur l'instance pour insérer des enregistrements dans la table d'incidents. Le champ de description renseignera les short_description sur l'incident.

```
<data>
   <record>
      <name>'Test Record 1'</name>
      <description>'Test Record 1 Description'</description>
      <tag>critical</tag>
   </record>
   <record>
      <name>'Test Record 2'</name>
      <description>'Test Record 2 Description'</description>
      <tag>security</tag>
   </record>
</data>
```

L'action de règle de chiffrement suivante peut s'appliquer :

```
function sampleXmlAction1() {
   var xmlContent = request.getAsXmlContent();
   // This loop iterates over all description tags that match the given path
   var xmlElementIterator = xmlContent.getIterator('data/record/description');
   while (xmlElementIterator.hasNext()) {
      var xmlElement = xmlElementIterator.next();
      xmlElement.valueFor('incident', 'short_decription');
   }
}
```

Cette action itère les balises de **description** et demande au serveur proxy de chiffrer les valeurs et de les insérer dans incident.short_description sur l'instance.

Remarque :
Cette règle trouve toutes les balises **de description** dans toutes les balises **d'enregistrement** de la charge utile XML. S'il n'y a qu'une seule occurrence d'une balise à chiffrer, la règle utilise toujours la structure xPath et itérateur. Cependant, il n'itére qu'une seule fois dans la boucle.

Mappage à un champ de table inconnu sur l'instance

Dans cet exemple, la règle itère sur les balises **d'enregistrement** , mais ne sait pas à quelles balises s'attendre dans la balise **d'enregistrement** . La seule chose connue est que les balises dans les balises **d'enregistrement** correspondent aux noms des colonnes spécifiées dans le paramètre URL de table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La règle spécifie également que, si la table est incidente, les données de la balise de **description** doivent être chiffrées et stockées dans le champ short_description de l'instance.

```
function sampleXmlAction2() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //Then, iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
      var field = fieldIterator.next();
      var fieldName = childElement.getName();
      //if table is incident, then description is encrypted for the short_description field
      if (tableName == 'incident' && fieldName == 'description') {
         field.valueFor(tableName, 'short_description');
      } else {
         //if table is not incident, ask the proxy to check if the given field is encrypted for the
 given table
         field.valueFor(tableName, fieldName);
      }
   }
}
```

Dans la fonction *`encryptFieldsInRecord(),`* la méthode *`valueFor()`* est appelée sur une table et un champ qui sont affectés dynamiquement en fonction de la demande. Même si les noms de table et de champ peuvent changer, la règle demande au proxy de vérifier si le champ de la table doit être chiffré en fonction des configurations de chiffrement définies.

Si le champ n'est pas configuré pour le chiffrement ou si la balise ne correspond pas à un champ de la table, le proxy ignore cette balise. Si la balise correspond à un champ marqué pour le chiffrement, le Chiffrement Edge serveur proxy chiffre la valeur.

Utilisation d'une requête codée

Dans cet exemple, toutes les balises ont l'attribut **filter** , qui indique si la balise contient une requête codée.

```
<data>
   <record>
      <name filter="false">'Test Record 1'</name>
      <description filter="false">'Test Record 1 Description'</description>
      <query filter="true">category=1^name=edge</query>
   </record>
   <record>
      <name filter="false">'Test Record 2'</name>
      <description filter="false">'Test Record 2 Description'</description>
      <query filter="true">category=2^severity=3</query>
  </record>
</data>
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'action de règle de chiffrement suivante peut s'appliquer :

```
function sampleXmlAction3() {
  var xmlContent = request.getAsXmlContent();
  var tableName = request.urlParam.table;
  // This first iterator will iterate over all record elements
  var xmlElementIterator = xmlContent.getIterator('data/record');
  while (xmlElementIterator.hasNext()) {
     encryptFieldsInRecord(xmlElementIterator.next());
  }
}
function encryptFieldsInRecord(xmlElement) {
  //this time we want to iterate over all tags representing fields in the table
  var fieldIterator = xmlElement.getIteratorOverAllChildren();
  while (fieldIterator.hasNext()) {
     var field = fieldIterator.next();
     var fieldname = childElement.getName();
     //let's look at the filter attribute, if true, then encrypt as encoded query
     if (field.getAttributeValue('filter') == 'true') {
        field.encodedQueryFor(tableName);
     } else {
        //if it is false then check if the field should be encrypted
        field.valueFor(tableName, fieldName);
     }
  }
}
```

Si la valeur de **l'attribut de filtre** est définie sur vrai, la règle demande au serveur proxy de chiffrer les valeurs de la requête codée. Si faux, la règle demande au proxy de vérifier si le champ doit être chiffré.

XMLContent

Objet global qui fournit des méthodes pour itérer sur le contenu XML.

Vous pouvez accéder à un objet *`XMLContent`* en appelant getAsXmlContent() sur un objet *de demande* .

Vous accédez aux données XML dans un paramètre POST ou URL en appelant request.postParams.<nom du paramètre>.getAsXmlContent() ou request.urlParams.<nom du paramètre>.getAsXmlContent().

XMLContent : getIterator()

Renvoie un objet *`XMLElementIterator pour le contenu XML.`*

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet *`XMLContent`* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

XMLContent : getIterator(String xPath)

Renvoie un objet `XMLElementIterator` pour le contenu XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
xPath	Chaîne	Expression de type xPath qui spécifie l'emplacement de démarrage dans l'objet `XMLContent` .

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLContent` .

XMLElementIterator

Fournit des méthodes pour itérer sur des éléments XML.

Vous obtenez un objet `XMLElementIterator` en appelant la méthode `getIterator()` de la classe `XMLContent` .

XMLElementIterator : hasNext()

Détermine s'il existe un autre élément disponible.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Booléen	Vrai si un autre élément est disponible.

XMLElementIterator : next()

Renvoie l'élément suivant dans l'itérateur.

Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLElement	L'élément XML suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

XMLElement

Fournit des méthodes pour itérer à travers des éléments XML et mapper des valeurs aux champs d'une table.

Vous obtenez un objet `XMLElement` en appelant la méthode `next()` d'un objet `XMLElementIterator` .

XMLElement : getIterator(String xPath)

Renvoie un objet `XMLElementIterator` pour l'élément XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
xPath	Chaîne	Une expression de type xPath qui spécifie où commencer dans l'objet `XMLElement` .

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLElement` .

XMLElement : getIteratorOverAllChildren()

Renvoie un objet `XMLElementIterator` qui inclut tous les sous-éléments de l'élément XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLElement` .

XMLElement : valueFor(String tableName, String fieldName)

Spécifie que la valeur de l'élément est mappée au champ spécifié dans la table spécifiée.

L'appel de cette méthode sur une valeur d'élément indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré. Si les noms de table et de champ sont inconnus, vous pouvez appeler la méthode `valueFor()` sur une table et un champ qui sont affectés dynamiquement en fonction de la demande.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoie

Type	Description
nul	

XMLElement : encodedQueryFor(String tableName)

Spécifie que la valeur de l'élément est une requête codée pour la table spécifiée.

L'appel de cette fonction sur un élément indique au proxy que la valeur de l'élément est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les champs de la requête codée qui doivent être chiffrés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous prévoyez que la requête s'exécute.

Renvoie

Type	Description
nul	

XMLElement : getName()

Renvoie le nom de l'élément.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Nom de l'élément.

XMLElement : getAttributeValue(attribut de chaîne)

Renvoie la valeur de l'attribut spécifié.

Paramètres

Nom	Type	Description
attribut	Chaîne	Nom d'attribut.

Renvoie

Type	Description
Chaîne	Valeur de l'attribut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

API JSON

Les API JSON peuvent être utilisées après l'appel de `getAsJsonContent()sur l'objet` de demande ou une propriété `ParameterValue` .

Lorsque vous utilisez des API JSON pour écrire votre règle de chiffrement, vous pouvez suivre un format général :

1. `Appelez getAsJsonContent()` sur l'objet de la `demande`. Cela renvoie un objet itérable de la classe sous-jacente `JsonNode` .
2. Appelez `iterator()` ou `getIterator(String xPath)` sur l'objet `JsonNode` . Cela renvoie un objet `JsonNodeIterator` qui peut être utilisé pour itérer sur les nœuds de l'objet JSON.
3. Appelez la méthode `hasNext()` sur l'objet `JsonNodeIterator` pour déterminer si un autre élément est disponible.
4. Appelez `next()` sur l'objet `JsonNodeIterator` pour renvoyer l'élément JSON suivant. Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`
5. Appelez `valueFor(String tableName, String fieldName)` sur l'élément JSON. Cette méthode indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

> **Remarque :**
> Pour déterminer si vous souhaitez appeler `valueFor(String tableName, String fieldName)` sur un élément JSON, vous pouvez utiliser la méthode `getName()` pour renvoyer le nom de l'élément.

Mappage à un champ de table connu sur l'instance

Dans cet exemple, la charge utile JSON est traitée sur l'instance pour insérer des enregistrements dans la table d'incidents. Le champ de description renseigne les short_description sur l'incident.

```
{
   data: {
      records: [
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         },
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         }],
      "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
   },
   "source": "10.11.13.14"
}
```

La règle suivante peut s'appliquer :

```
function sampleJsonAction1() {
   var jsonContent = request.getAsJsonContent();
   // This loop iterates over all description elements in the records array
   var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        jsonNode.valueFor('incident', 'short_decription');
    }
}
```

Cette action itère à travers les nœuds de **description** et demande au serveur proxy de chiffrer les valeurs et de les insérer dans incident.short_description sur l'instance.

Remarque :
Cette règle trouve tous les nœuds de **description** dans la charge utile JSON. S'il n'y a qu'une seule occurrence d'un nœud à chiffrer, la règle utilise toujours xPath et la structure de l'itérateur. Cependant, il n'itére qu'une seule fois dans la boucle.

Mappage à un champ de table inconnu sur l'instance

Dans cet exemple, la règle itère sur les **enregistrements**, mais ne sait pas à quels nœuds s'attendre. La seule certitude est que pour chaque objet dans les **enregistrements**, les nœuds correspondent aux noms des colonnes spécifiées dans le paramètre URL de la table.

La règle spécifie également que, si la table est incidente, les données du nœud de **description** doivent être chiffrées et stockées dans le champ short_description de l'instance.

```
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
            encryptFieldsInRecord(jsonNodeIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            if (fieldName == 'description') {
                field.valueFor(tableName, 'short_description');
            } else {
                field.valueFor(tableName, fieldName);
            }
    }
}
```

Dans la fonction `encryptFieldsInRecord()`, la méthode `valueFor()` est appelée sur une table et un champ qui sont affectés dynamiquement en fonction de la demande. Même si les noms de table et de champ peuvent changer, la règle demande au proxy de vérifier si le champ de la table doit être chiffré en fonction des configurations de chiffrement définies.

Si le champ n'est pas configuré pour le chiffrement ou si le nom de nœud ne correspond pas à un champ de la table, le proxy ignore ce nœud. Si le nom du nœud correspond à un champ marqué pour chiffrement, le proxy chiffre la valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation d'une requête codée

```
function sampleJsonAction3() {
   var jsonContent = request.getAsJsonContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var jsonNodeIterator = jsonContent.getIterator('data');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
      if (jsonNode.getName() == 'records')
         encryptRecors(jsonNodeIterator.next());
      else if (jsonNode.getName() == 'query')
         jsonNode.encodedQueryFor(tableName);
   }
}
function encryptRecords(jsonNode) {
   //we iterate over all fields in the node
   var recordIterator = jsonNode.iterator();
   while (recordIterator.hasNext()) {
      encryptFieldsInRecord(recordIterator.next());
   }
}
function encryptFieldsInRecord(jsonNode) {
   //this time we want to iterate over all nodes
   var fieldIterator = jsonNode.iterator();
   while (fieldIterator.hasNext()) {
         var field = fieldIterator.next();
         var fieldname = childElement.getName();
         field.valueFor(tableName, fieldName);
   }
}
```

Dans cet exemple, la règle itère sur les **données**. Lorsqu'il trouve **des enregistrements**, il exécute la même logique que dans le deuxième exemple, en itérant sur les champs de chaque nœud. Lorsqu'il trouve le nœud de **requête** , il appelle `encodedQueryFor()` pour chiffrer les valeurs qui doivent être chiffrées dans la requête.

Nœud JSON

Objet global qui fournit des méthodes pour itérer sur le contenu JSON.

Vous pouvez accéder à un objet `JsonNode` en appelant getAsJsonContent() sur un objet *de demande* .

Vous accédez au contenu JSON à partir d'un paramètre POST ou URL en appelant request.postParms.<nom de paramètre >.getAsJsonContent() ou request.urlParms.<nom de paramètre >.getAsJsonContent().

JsonNode : getIterator(String xPath)

Renvoie un objet `JsonNodeIterator` pour le contenu JSON.

Cette méthode ne peut être utilisée que sur le nœud racine, mais peut être utilisée pour pénétrer profondément dans l'objet JSON. Les traversées suivantes doivent utiliser la méthode *`iterator(`*).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
xPath	Chaîne	Une expression xPath.

Renvoie

Type	Description
JsonNodeIterator	Objet qui peut itérer sur les nœuds de l'objet JSON.

JsonNode : iterator()

Renvoie un objet `JsonNodeIterator` qui itère sur tous les nœuds enfants du nœud actuel.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
JsonNodeIterator	Objet qui peut itérer sur les nœuds de l'objet JSON.

JsonNode : getAsString()

Renvoie la valeur du nœud actuel sous forme de chaîne.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Valeur de nœud actuelle.

JsonNode : getAsString(String propertyName)

Renvoie la valeur de chaîne de la propriété spécifiée.

Paramètres

Nom	Type	Description
propertyName	Chaîne	Nom de la propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoie

Type	Description
Chaîne	Valeur de la propriété.

JsonNode : getName()

Renvoie le nom du nœud JSON actuel.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Nom du nœud JSON actuel.

JsonNode : valueFor(String tableName, String fieldName)

Spécifie que la propriété JSON est mappée au champ spécifié dans la table indiquée.

L'appel de cette méthode sur une propriété JSON indique au proxy que la valeur de cette propriété est mappée au champ spécifié dans la table spécifiée. Le proxy décide ensuite si le champ doit être chiffré. Si les noms de table et de champ sont inconnus, vous pouvez appeler la méthode `valueFor()` sur une table et un champ qui sont affectés dynamiquement en fonction de la demande.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Renvoie

Type	Description
nul	

JsonNode : encodedQueryFor(String tableName)

Spécifie que la valeur de la propriété JSON est une requête codée pour la table spécifiée.

L'appel de cette fonction sur un nœud JSON indique au proxy que la valeur est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les valeurs des champs de la requête codée qui doivent être chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous prévoyez que la requête s'exécute.

Renvoie

Type	Description
nul	

JsonNodeIterator

Vous obtenez un objet `JsonNodeIterator` en appelant les méthodes `getIterator()` ou `iterator()` de la classe `JsonNode` .

JsonNodeIterator : hasNext()

Détermine s'il existe une autre propriété disponible.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Booléen	True si une autre propriété est disponible.

JsonNodeIterator : next()

Renvoie la propriété suivante dans l'itérateur.

Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	Le `prochain JsonNode`.

print(Message de chaîne)

Imprime un message dans le fichier journal de la couche : <répertoire du serveur proxy>/logs/wrapper_<date>.log.

Cette méthode est disponible uniquement dans un script d'action de Chiffrement Edge règle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
message	Chaîne	Message à écrire dans le fichier journal de la couche.

Renvoie

Type	Description
nul	

Mots clés interdits

Le Chiffrement Edge proxy valide les scripts de règle de chiffrement avant d'enregistrer la règle. De nombreux mots clés JavaScript ne sont pas autorisés dans les scripts de règles de chiffrement.

Mots clés interdits

Mot clé
__DIR__
__LIME__
__LIGNE__
__parent__
__proto__
Erreur
Eval
getClass
getPrototypeOf
Java
Java X
JAVAFX
Importateur Java
charger
loadWithNewGlobal
nouveau
Packages
Objet
prototype
ExpEnr
setPrototypeOf
ce

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés interdits (suite)

Mot clé
jeter

Attributs du dictionnaire Chiffrement Edge

Ajoutez des attributs de dictionnaire aux tables et aux champs pour contrôler leur fonctionnement avec Chiffrement Edge.

Pour définir un attribut de dictionnaire sur true, vous devez saisir `attribute=true` dans le champ **Attributs** . Pour ajouter un attribut de dictionnaire à un enregistrement, reportez-vous à la section Altering tables and fields using dictionary attributes .

Chiffrement Edge exclu [edge_encryption_excluded]

Détermine si le champ est exclu du chiffrement.

Lorsque la valeur est définie sur `vrai`, le champ ou la table ne peut pas être chiffré. Lorsque la valeur est définie sur `faux`, le champ peut être chiffré.

- Valeur : vrai/faux
- Élément cible : champ ou table
- Valeur par défaut : false

Chiffrement Edge activé [edge_encryption_enabled]

Détermine si le champ est éligible au chiffrement via une configuration de chiffrement.

Lorsque la valeur est définie sur `vrai`, le champ est éligible au chiffrement. Lorsque la valeur est définie sur `faux`, le champ n'est pas éligible au chiffrement. Étant donné que cet attribut est utilisé par le système et ne peut pas être modifié, il n'est pas affiché à l'utilisateur.

Remarque :
Cet attribut n'indique pas qu'un champ est chiffré et ne déclenche aucune logique de chiffrement sur le champ. L'attribut détermine plutôt la possibilité que le champ soit chiffré par un utilisateur.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : true pour les champs Chaîne

Texte clair Chiffrement Edge autorisé [edge_encryption_clear_text_allowed]

Détermine si les scripts côté serveur peuvent ajouter des données non chiffrées à une chaîne chiffrée dans le champ pour les actions utilisateur effectuées via le serveur proxy ou tout script automatisé côté serveur, telles que les travaux planifiés.

Lorsque la valeur est définie sur `vrai`, l'ajout de données est autorisé. Lorsque la valeur est définie sur `faux`, l'ajout de données n'est pas autorisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : faux

Séparation de domaine et Chiffrement Edge

Séparation de domaine est prise en charge dans des circonstances limitées avec Chiffrement Edge. Chiffrement Edge fournit la possibilité de chiffrer des données à partir de l'environnement du client via l'utilisation de configurations, de règles et de clés spécifiques définies sur le Chiffrement Edge proxy. Le proxy n'est Chiffrement Edge pas sensible au domaine et ne peut pas prendre en charge les paramètres spécifiques à un domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Aucun

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique métier pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Fonctionnement de Séparation de domaine dans Chiffrement Edge

Chiffrement Edge peut être utilisé lorsque des clés, des configurations et des règles spécifiques à un domaine ne sont pas requises.

Information associée

Séparation de domaine pour les fournisseurs de services

Intégration de données avec Chiffrement Edge

Pour intégrer des données tierces à une instance à l'aide Chiffrement Edge de , vous devez acheminer les données via le serveur proxy à l'aide d'intégrations Chiffrement Edge prises en charge. Les intégrations prises en charge utilisent des règles de chiffrement du système de base qui mappent les données de chaque charge utile aux champs d'une table.

Charger des données dans des champs marqués pour chiffrement

Chiffrement Edge ne prend pas en charge l'importation ou l'exportation de données vers des champs Excel, CSV, XML ou d'autres types de fichiers vers ou depuis des champs avec des configurations de chiffrement définies.

ODBC driver

Chiffrez les demandes et interrogez les données via le serveur proxy à l'aide Chiffrement Edge du pilote ODBC.

Pour en savoir plus : Intégration du pilote ODBC Chiffrement Edge

MID Server

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez configurer l'acheminement des Serveur MID données via un Chiffrement Edge serveur proxy. Cependant, certaines restrictions s'appliquent.

Pour en savoir plus : Intégration du Serveur MID Chiffrement Edge

Services web REST/SOAP

Utilisez les services web REST/SOAP pour mettre à jour ou récupérer les données d'enregistrement via le Chiffrement Edge serveur proxy.

Pour en savoir plus : Services Web

Service web JSONv2

Utilisez les API de service Web JSONv2 pour mettre à jour ou récupérer les données d'enregistrement via le Chiffrement Edge serveur proxy. Les règles de chiffrement du système de base prennent en charge les API de récupération et de modification de données.

- Pour insérer un seul enregistrement à l'aide de l'API de modification de données, utilisez les méthodes `insert()` ou `insertMutiple()`.
- Pour insérer plusieurs enregistrements à l'aide de l'API de modification de données, utilisez la méthode `insertMultiple()`.

Informations complémentaires : Service Web JSONv2

Pour chiffrer les données à partir d'intégrations tierces personnalisées non répertoriées ci-dessus, créez des règles de chiffrement personnalisées. Voir Définir une règle de chiffrement personnalisée.

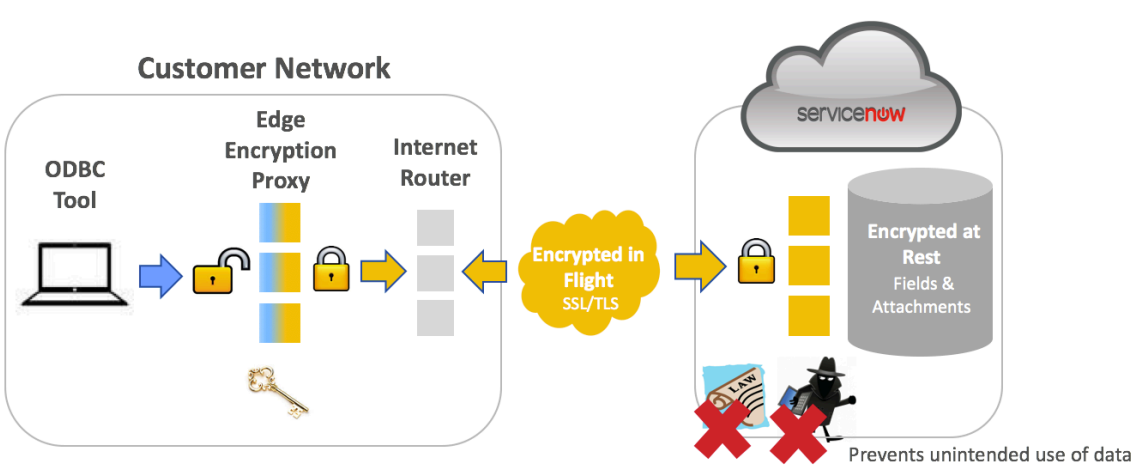
Charger des pièces jointes dans des enregistrements marqués pour chiffrement

Les pièces jointes peuvent être téléchargées dans des tables avec le chiffrement des pièces jointes configuré à l'aide des services Web REST et SOAP.

Intégration du pilote ODBC Chiffrement Edge

Configurez votre pilote ODBC pour interroger les données chiffrées par Chiffrement Edge. Le Chiffrement Edge serveur proxy chiffre les demandes du pilote ODBC à l'instance lorsqu'il ServiceNowChiffrement Edge est intégré au pilote ODBC.

Les réponses chiffrées de l'instance sont déchiffrées via le Chiffrement Edge serveur proxy avant d'être transmises au pilote ODBC de votre réseau.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour une intégration réussie, le pilote ODBC doit approuver le certificat du Chiffrement Edge serveur proxy. Si le certificat du Chiffrement Edge serveur proxy est signé par une autorité de certification approuvée par le pilote ODBC, le Chiffrement Edge serveur proxy est automatiquement approuvé. Toutefois, si une autorité de certification approuvée par le pilote ODBC n'a pas signé le certificat du Chiffrement Edge serveur proxy, vous devez importer le certificat auto-signé dans le magasin de clés de confiance ODBC.

Importez un certificat autosigné dans le magasin de clés de confiance ODBC

Si une autorité de certification approuvée par le pilote ODBC n'a pas signé le certificat du Chiffrement Edge serveur proxy, vous devez importer un certificat auto-signé dans le magasin de clés de confiance ODBC. Vous pouvez exporter le certificat à partir du Chiffrement Edge serveur proxy et l'importer dans le magasin de clés de confiance ODBC.

Avant de commencer
Rôle requis : admin

Pour déterminer si une autorité de certification approuvée par le pilote ODBC a signé le certificat du Chiffrement Edge serveur proxy, exécutez la commande suivante dans le répertoire keystore du répertoire de base du proxy pour afficher une liste des autorités de certification approuvées par le pilote ODBC :

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

Remarque :

Dans la plupart des cas, le client se connecte aux Chiffrement Edge proxys via un équilibreur de charge, de sorte que le certificat serait le certificat configuré dans l'équilibreur de charge.

Dans le cas où il n'y a pas d'équilibreur de charge entre le client et le serveur proxy Edge, le certificat est le certificat présenté par le proxy Edge et est configuré dans le *`edgeencryption.properties`* fichier.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Pour plus d'informations sur la modification des propriétés, consultez Configurer des propriétés supplémentaires dans le fichier de propriétés de Chiffrement Edge

Procédure

1. Accéder au répertoire keystore dans le répertoire de base du proxy.
2. Vérifiez le magasin de clés du certificat auto-signé.
   a. Pour vérifier la présence du certificat dans le magasin de clés, vous pouvez exécuter la commande suivante pour répertorier tous les éléments du magasin de clés.

      ```
      keytool -list -keystore keystore.jceks -storetype jceks -v
      ```

   b. Localisez l'alias de clé dans la liste d'éléments.
3. À l'aide de l'alias de clé, exportez le certificat vers un fichier .cer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file
 name>.cer
```

4. Accédez à votre répertoire de magasin de clés de confiance ODBC : ODBC\ip\Java\jre\lib\security \cacerts.
5. Importez le certificat dans votre magasin de clés de confiance ODBC.

```
keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
```

Définir les propriétés du pilote ODBC

Définissez les propriétés du pilote ODBC pour acheminer les demandes via le Chiffrement Edge serveur proxy.

Avant de commencer

Rôle requis : admin

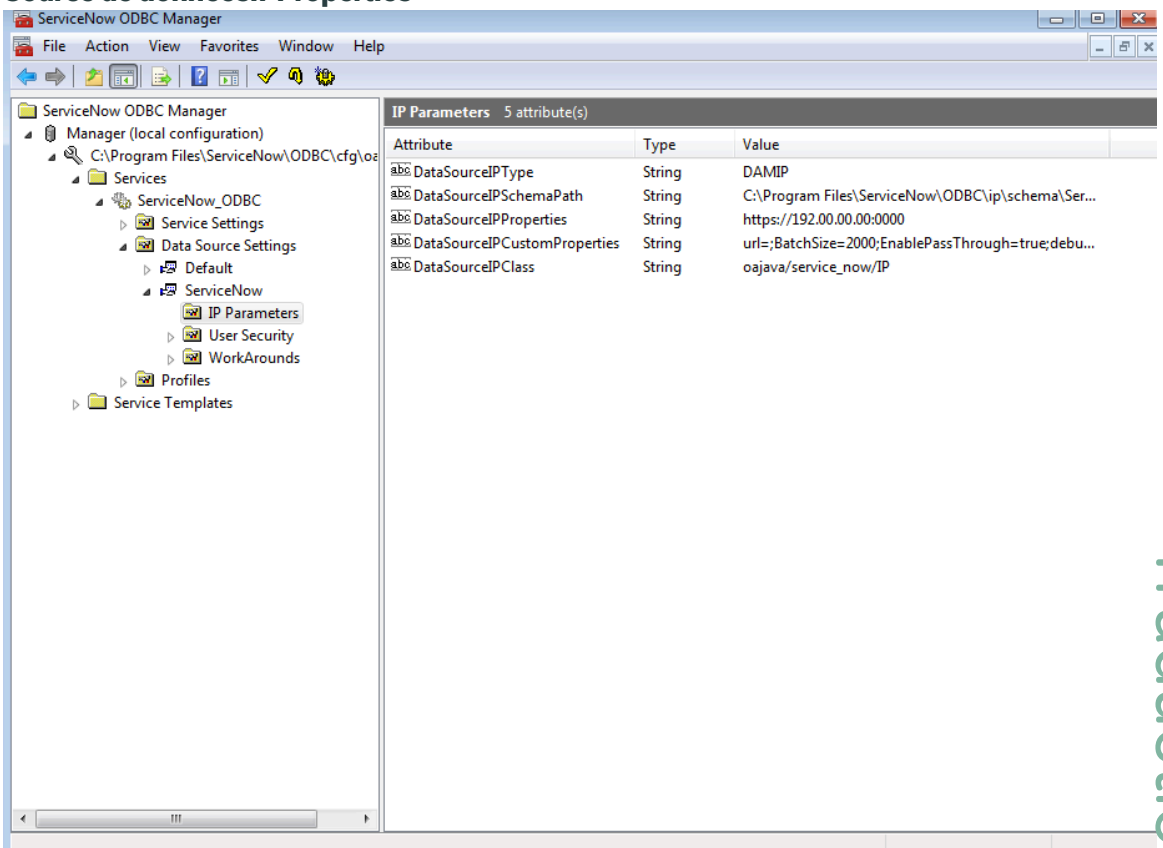
Procédure

1. Sous Windows, accédez à **Début** > **Programmes** > **Console de gestion ODBC ServiceNow**.
2. Développez la racine de l'arborescence de la console comme suit : ServiceNow ODBC Manager \Manager\<emplacement d'installation>\Services\ServiceNow_ODBC\Paramètres de source de données\ServiceNow\Paramètres IP.
3. Double-cliquez sur l'attribut **DataSourceIPProperties** .
4. Remplacez la **valeur** par l'URL de votre serveur proxy Chiffrement Edge, par exemple https://<adresse IP > :<port>

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source de donnéesIPProperties



5. Cliquez sur **OK**.

Que faire ensuite

Le pilote ODBC est maintenant configuré pour acheminer les demandes vers l'instance via le Chiffrement Edge serveur proxy.

Intégration du Serveur MID Chiffrement Edge

Configurez le pour acheminer les Serveur MID données via un Chiffrement Edge serveur proxy.

Lorsqu'il est intégré à , Serveur MID le Chiffrement Edge serveur proxy agit comme le point de Serveur MID terminaison de . Le Chiffrement Edge serveur proxy crypte et déchiffre ensuite les données qui transitent entre l'instance et le ServiceNowServeur MID serveur .

Limitations lors de l'intégration au serveur MID

Lorsque Serveur MID les données sont configurées pour passer par le Chiffrement Edge serveur proxy, les limitations suivantes s'appliquent :

- Le chiffrement des champs de file d'attente ECC n'est pas pris en charge.
- Les données chiffrées ne peuvent pas être utilisées avec Découverte ou Mappage des services.

Pointez le serveur MID vers le serveur proxy Chiffrement Edge

Pour transmettre des données via le Chiffrement Edge serveur proxy, mettez à jour le Serveur MID fichier de Serveur MID configuration pour qu'il pointe vers Serveur MID le Chiffrement Edge serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Lors de la configuration pour qu'il Serveur MID passe par le Chiffrement Edge serveur proxy, vous ne pouvez pas utiliser les propriétés du proxy Web dans le Serveur MID fichier de configuration pour acheminer le trafic via le Chiffrement Edge serveur proxy vers votre instance. Au lieu de cela, vous devez définir le Chiffrement Edge serveur proxy comme point de Serveur MID terminaison de .

Procédure

1. Accédez à votre répertoire local Serveur MID et ouvrez le fichier config.xml .
2. Recherchez l'élément <parameter name="url » value="https ://YOUR_INSTANCE.service-now.com » /> et remplacez la propriété value par l'URL de votre Chiffrement Edge serveur proxy.
   Par exemple, http://hostname.mycompany.com:8081
   Cette étape demande Serveur MID de transmettre le Chiffrement Edge trafic au serveur proxy au lieu de l'instance. Le Chiffrement Edge serveur proxy chiffre à son tour tous les champs nécessaires et transmet la charge utile à l'instance.
3. Enregistrez et fermez le fichier.
4. En cas d'exécution, redémarrez le Serveur MID.

Diagnostics et performances de Chiffrement Edge

Surveillez les Chiffrement Edge tendances des performances des serveurs proxy et explorez les erreurs générées par le Chiffrement Edge serveur proxy.

Performance du proxy Edge

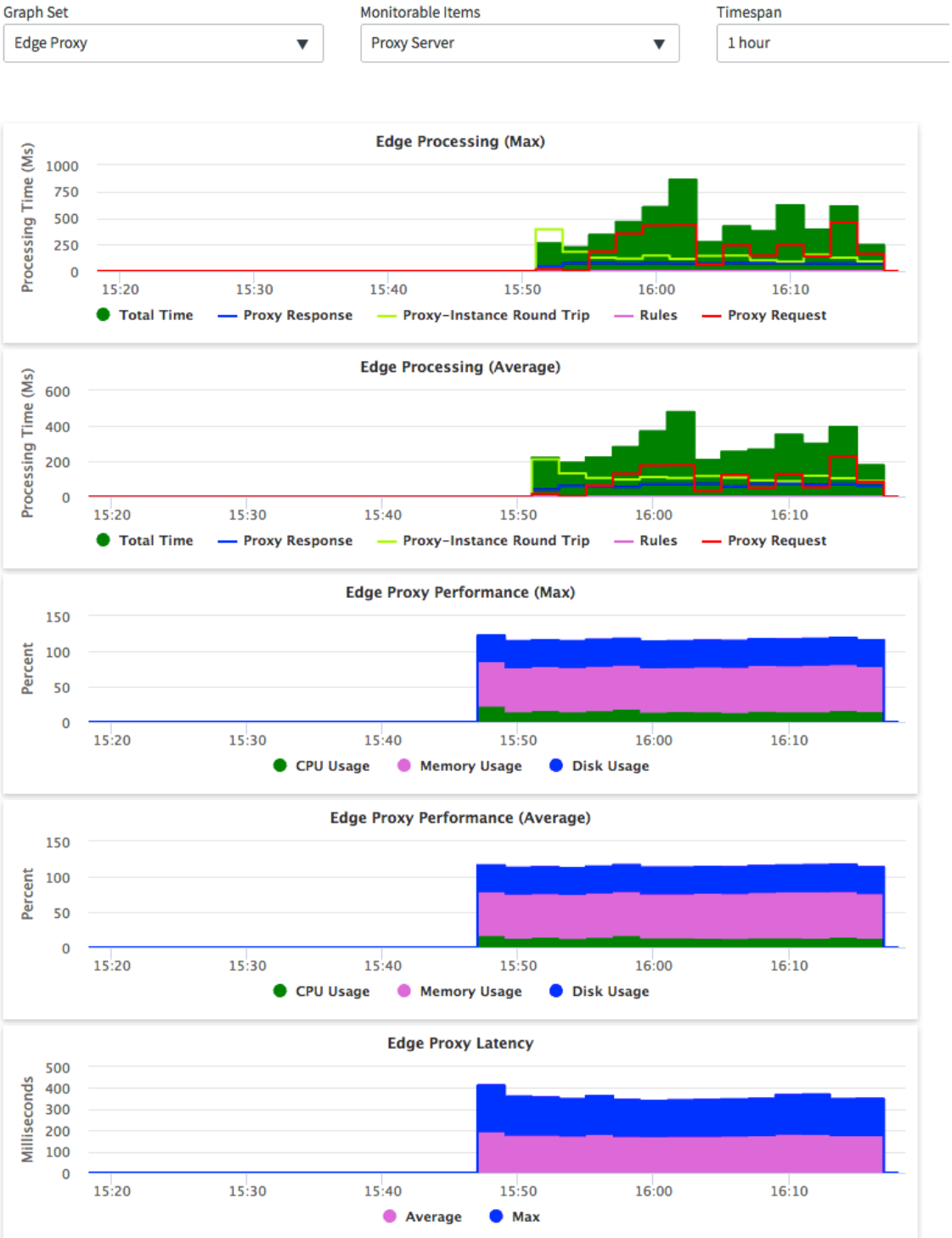
Affichez les principales Chiffrement Edge tendances des performances des serveurs proxy à l'aide du graphique Proxy Edge défini sur la page d'accueil Performance ServiceNow . Les tendances surveillées sont les suivantes :

- Délais de réponse maximum et moyen entre le client, le serveur proxy et l'instance.
- Utilisation du processeur, de l'espace disque et de la mémoire de l'ordinateur hôte.
- Latence réseau maximale et moyenne entre le serveur proxy et l'instance ServiceNow .

Remarque :
Chiffrement Edge Les serveurs proxy avec des noms en double ne signalent pas les tendances de performance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traitement Edge (max et moyenne)

Temps maximal et moyen, en millisecondes, pour traiter une demande. Ces points de données sont des tendances générales dans le temps.

- **Durée totale** : temps nécessaire au serveur proxy pour recevoir une demande d'un client et envoyer une réponse. Ce point de données est la somme des points de données suivants.
- **Réponse proxy** : délai de traitement par le serveur proxy d'une réponse de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Aller-retour** entre instances proxy : temps auquel le serveur proxy envoie une demande à l'instance et reçoit une réponse. Inclut la latence réseau entre le serveur proxy et l'instance et le temps consacré par l'instance au traitement de la demande.
- **Règles** : temps nécessaire au serveur proxy pour évaluer une demande à l'aide de règles de chiffrement définies.
- **Demande proxy** : temps nécessaire au serveur proxy pour traiter une demande client et la transmettre à l'instance.

Performances du proxy Edge (max et moyen)

Pourcentage maximal et moyen de ressources utilisées sur l'ordinateur hôte.

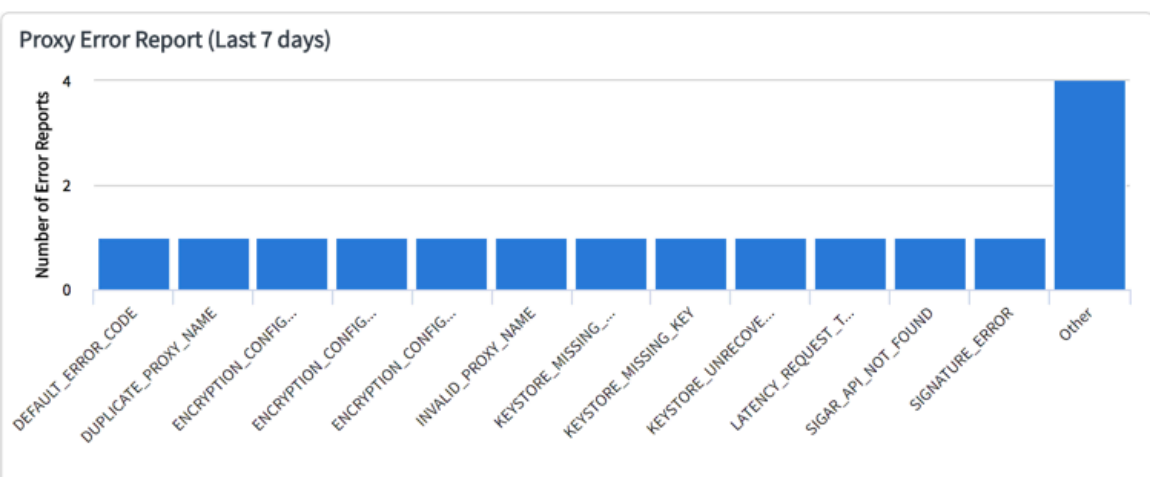
- Utilisation du processeur
- Utilisation de la mémoire
- Utilisation du disque

Latence du proxy de périphérie

Latence réseau maximale et moyenne en millisecondes à un moment donné. La latence est déterminée par le temps d'aller-retour nécessaire pour qu'un serveur proxy envoie un simple ping à l'instance et reçoive une réponse.

Rapports d'erreurs de proxy

Accédez à la **Configuration de Chiffrement Edge** > **Diagnostics et dépannage** > **Rapports d'erreurs de proxy** pour afficher toutes les erreurs de serveur proxy collectées au cours des sept derniers jours.



Les erreurs sont collectées sur une période d'une minute. Chaque minute, un rapport d'erreur est généré. L'axe vertical affiche le nombre de rapports d'erreurs au cours des sept derniers jours qui incluent chaque erreur. Par exemple, même si l'erreur DEFAULT_ERROR_CODE est renvoyée plusieurs fois sur une période d'une minute, la barre de DEFAULT_ERROR_CODE n'atteindra qu'une seule sur **l'axe Nombre de rapports d'erreurs** .

À partir de cette vue, vous pouvez :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur chaque barre de code d'erreur de proxy pour afficher le rapport sur une erreur unique pour chaque serveur proxy. À partir de cette vue, vous pouvez cliquer à nouveau sur la barre pour afficher le texte d'erreur dans la Chiffrement Edge table Proxy Stat [edge_encryption_stat]. Suivez les liens dans le texte d'erreur pour voir plus d'informations et les étapes de rattrapage possibles.
- Cliquez sur **Autre** pour afficher la page deux du rapport d'erreurs.

Remarque :
Si vous avez plusieurs serveurs proxy portant le même nom, une seule erreur DUPLICATE_PROXY_NAME apparaît dans le rapport d'erreur du proxy. Aucune autre erreur n'est signalée pour les serveurs proxy avec des noms en double. Si vous rencontrez cette erreur, assurez-vous que tous les serveurs proxy ont des noms uniques.

Ressources supplémentaires en matière de surveillance

L'instance suit tous les proxys de chiffrement. Chaque Chiffrement Edge serveur proxy s'enregistre au démarrage. L'instance est notifiée lorsque :

- Un nouveau Chiffrement Edge serveur proxy démarre.
- Un Chiffrement Edge serveur proxy est arrêté intentionnellement.

Si un Chiffrement Edge serveur proxy tente de s'enregistrer auprès d'une instance qui n'est Chiffrement Edge pas installée, le proxy ne démarre pas.

Tous les fichiers de configuration de chiffrement sont audités. Les enregistrements supprimés sont audités sur tous les fichiers de configuration de chiffrement. Les enregistrements d'audit sont placés dans la table sys_audit. Pour afficher l'historique d'un enregistrement de configuration spécifique, affichez l'enregistrement, puis cliquez sur **Historique** > **Liste** dans le menu. La tâche de chiffrement en masse n'est pas auditée.

Utilisez les ressources supplémentaires suivantes pour surveiller vos serveurs proxy.

Table	Description
Tentatives d'insertion non valides [sys_edge_encryption_invalid_insert_log]	Liste des tentatives d'enregistrement des données suivantes dans des champs chiffrés : • Données non chiffrées. • Données qui ne proviennent pas d'un Chiffrement Edge proxy. L'instance rejette, puis consigne toute tentative d'enregistrement de ces données. Si vous disposez du rôle security-admin, vous pouvez afficher les journaux dans la liste Tentatives d'insertion non valides.
Échecs de tâches [sys_encryption_job_execution]	Une liste des tâches qui ne se sont pas exécutées avec succès.
Journaux système	L'instance vérifie périodiquement les messages de chaque serveur proxy enregistré. Si un serveur proxy n'a pas envoyé de message dans le délai requis, une erreur est consignée. Le message du journal contient des informations sur le proxy de chiffrement et la dernière fois que le proxy a envoyé une requête à l'instance. Si l'instance détermine

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	qu'aucun des proxys de chiffrement n'est en ligne, elle consigne un message. Ces messages sont ajoutés au journal système.

Désactiver ou réduire la collecte de statistiques du proxy Edge

Empêchez le serveur proxy d'envoyer des Chiffrement Edge statistiques du jeu de graphiques proxy Edge à la page d'accueil ServiceNow Performance ou réduisez la fréquence de collecte des statistiques.

Avant de commencer
Rôle requis : admin ou security_admin

Pourquoi et quand exécuter cette tâche
En ajoutant des propriétés dans le fichier de configuration edgeencryption.properties , vous pouvez :

- Désactivez l'ensemble de graphiques proxy Edge.
- Modifier l'intervalle pendant lequel les statistiques sont collectées par le Chiffrement Edge serveur proxy. Par défaut, les statistiques sont collectées toutes les 30 secondes.

Procédure

1. Dans le répertoire d'installation de votre serveur proxy, ouvrez le fichier de configuration edgeencryption.properties situé dans le dossier <répertoire d'installation>/conf/ .
2. Ajoutez l'un des Propriétés du serveur proxy Chiffrement Edge.
3. Redémarrez le serveur proxy.

Augmenter la journalisation de débogage pour le Chiffrement Edge proxy

Augmentez le niveau de journalisation pour interpréter les journaux et déboguer les problèmes avec le proxy.

Il existe actuellement trois options pour augmenter la journalisation des débogages dans le Chiffrement Edge proxy. Augmentez le niveau de journalisation pour déboguer les problèmes, fournissez à l'assistance technique des informations permettant d'examiner le problème grâce à des instructions de journal plus détaillées.

En fonction du problème en cours de débogage, configurez la journalisation des débogages de l'une des trois façons suivantes :

- Problèmes de débogage autres que la connectivité SSL
- Journalisation des mesures de minutage pour les demandes via le proxy
- Débogage des problèmes de connectivité SSL entre le proxy Chiffrement Edge et l'instance

Pour tous les tickets de débogage, vous pouvez afficher et interpréter les journaux dans votre propre entreprise ou ouvrir un incident pour obtenir une interprétation de ServiceNow l'assistance technique fournissant la description du problème et la façon dont il est reproduit.

Problèmes de débogage avec l'application autres que la Chiffrement Edge connectivité SSL

Utilisez cette méthode pour déboguer les problèmes de l'application Chiffrement Edge , sans arrêter ni redémarrer le proxy. Ces étapes augmentent le niveau de journalisation et aident à résoudre la cause première avec des instructions de journal plus détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Remarque :
Les modifications apportées au fichier $proxy_installation_location/conf/log4j2.properties sont prises en charge par le proxy dans les 60 secondes environ suivant vos modifications. Vous n'avez pas besoin de redémarrer les proxys.

Procédure

1. Dans le fichier $proxy_installation_location/conf/log4j2.properties , recherchez la ligne suivante.

```
logger.edge.level=info
```

2. Remplacez la ligne ci-dessus par ce qui suit :

```
logger.edge.level=debug
```

3. Enregistrez le changement.
   Cela peut prendre jusqu'à 60 secondes pour que le changement prenne effet, mais cela ne nécessite pas de redémarrage du proxy.
4. Reproduisez votre problème.
5. Vérifiez les instructions de journal de débogage associées à l'application dans le fichier $proxy_installation_location/logs/edgeencryption.log .

Résultats
Après avoir effectué le changement de propriété, vous pouvez voir des détails supplémentaires dans votre fichier $proxy_installation_location/logs/edgeencryption.log . Une fois le débogage terminé, rétablissez la modification apportée au fichier $proxy_installation_location/conf/log4j2.properties .

Journalisation des mesures de minutage pour les demandes via le proxy

Activez la journalisation des mesures de minutage pour ajouter une instruction de mesure pour chaque demande traitée par le Chiffrement Edge proxy. Chacune de ces instructions du journal de mesure de minutage contient des informations utiles sur la demande, telles que les durées de traitement et la règle de chiffrement utilisée.

Avant de commencer
Rôle requis : admin

Remarque :

Les paramètres de journalisation supplémentaires sont ajoutés au fichier $proxy_installation_location/conf/log4j2.properties . Les modifications apportées sont traitées dynamiquement par le proxy dans un délai d'environ une minute après les modifications apportées au fichier, de sorte que vous n'avez pas besoin de redémarrer les proxys.

Procédure

1. Modifiez le fichier $proxy_installation_location/conf/log4j2.properties en ajoutant les lignes suivantes à la fin du fichier

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Enregistrez le fichier.

Résultats

Une fois le fichier log4j.properties enregistré, les types de messages suivants apparaissent dans le fichier journal $proxy_installation_location/logs/edgenetwork.log pour les heures réseau.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375754
 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1 proxy_instance_round_trip=14
 proxy_response_processing_time=1 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo3Pjq6
G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Les valeurs des messages du journal sont les suivantes :

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT, PATCH,
 DELETE

client_request_received: The timestamp noting when the HTTP client request arrived at the
 Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process the request in
 milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge Encryption rules for the
 request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the request to the instance
 until the instance sent the response and was received by the edge proxy in milliseconds
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

proxy_response_processing_time: How long the Edge proxy took to process the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received the request from the client and returned the response to the client in milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request

Déboguer les problèmes de connectivité SSL entre le Chiffrement Edge proxy et l'instance

Utilisez cette méthode pour déboguer les problèmes de connectivité SSL entre le Chiffrement Edge proxy et votre instance, tels que l'échec de l'accès à l'instance via le proxy. Ces étapes augmentent la journalisation et aident à trouver les instructions de journal détaillées.

Avant de commencer

Rôle requis : admin

Remarque :
Le débogage de connectivité SSL n'est pertinent que lors du dépannage des problèmes de type de connectivité TLS. En pratique, ce n'est pas courant et rarement nécessaire.

Procédure

1. Arrêtez le serveur proxy.
2. Ajoutez la ligne suivante au fichier $proxy_installation_location/conf/wrapper.conf, qui est une propriété de démarrage Java :

   ```
   wrapper.java.additional.<next available number in sequence> = -Djavax.net.debug=all
   ```

   Par exemple :

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Enregistrez le changement et redémarrez le serveur proxy.
4. Reproduisez votre problème de connectivité.

Résultats

Après avoir reproduit le problème, les instructions du journal de débogage relatives à l'échange SSL se trouvent dans le fichier $proxy_installation_location/logs/wrapper_<current date>.log . Lorsque vous avez terminé le débogage. Vous pouvez supprimer à distance la journalisation supplémentaire en supprimant ou en commentant la ligne créée lors des étapes précédentes.

Chiffrement de la base de données

ServiceNow® propose des méthodes de chiffrement de base de données (DBE) et de chiffrement complet du disque pour les clients ayant des obligations légales en matière de protection des données qui peuvent nécessiter une protection au repos pour toutes les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
À partir de la Washington DC version, Chiffrement de base de données est en cours de préparation pour une dépréciation future. Cloud Encryption est la solution de remplacement du chiffrement des données au repos. Pour plus de détails, voir Chiffrement dans le cloud avec gestion des clés

Explorer	Demande	Référence
		
Découvrez les principales fonctionnalités et la valeur commerciale de Chiffrement de base de données.	En savoir plus sur la façon de demander la rotation de clé de base de données.	Le chiffrement de la base de données avec commutateur contrôlé par le client (DBE-CCS) est une solution de chiffrement qui chiffre toutes les données au repos lorsqu'elles ne sont pas utilisées dans la base de données.

Traduction automatique

Exploration du chiffrement de base de données

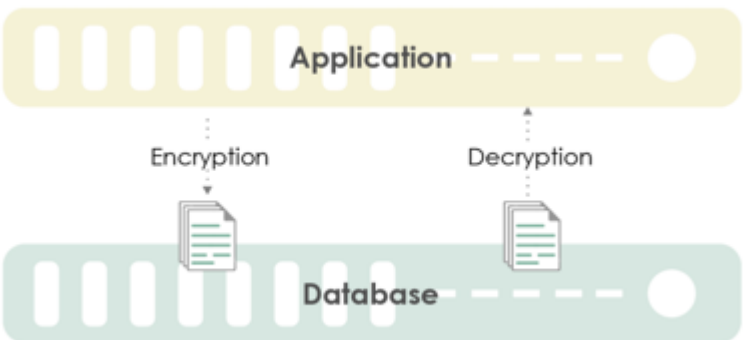
ServiceNow® propose des méthodes de chiffrement de base de données (DBE) et de chiffrement complet du disque pour les clients ayant des obligations légales en matière de protection des données qui peuvent nécessiter une protection au repos pour toutes les données.

Important :
À partir de la Washington DC version, Chiffrement de base de données est en cours de préparation pour une dépréciation future. Cloud Encryption est la solution de remplacement du chiffrement des données au repos. Pour plus de détails, voir Chiffrement dans le cloud avec gestion des clés

Le chiffrement de la base de données permet de protéger toutes les données avec un chiffrement AES-256 symétrique, que la base de données soit en ligne ou hors ligne. Du point de ServiceNow AI Platform vue, toutes les données sont déchiffrées.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

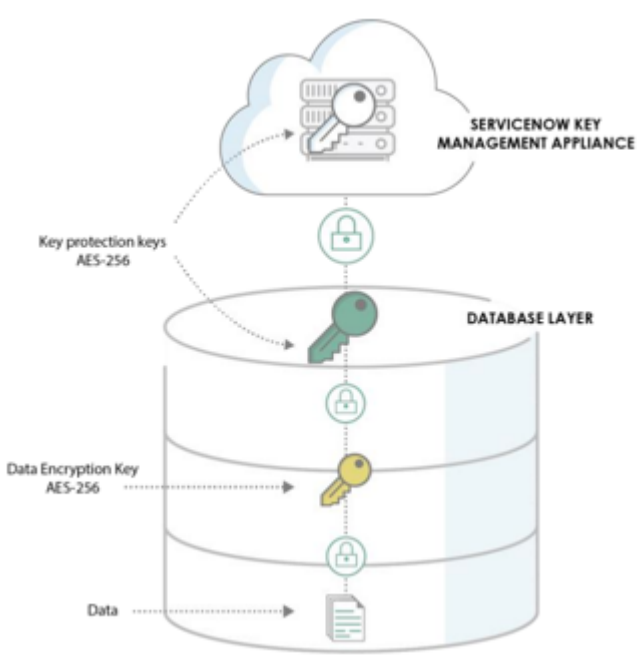
- Chiffrement de la base de données prend en charge le chiffrement de toutes les données stockées en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.
- Le chiffrement intégral du disque protège les données hors ligne en cas de perte ou de vol de disque.



Avec le chiffrement de base de données, toutes les données stockées sont chiffrées et les enregistrements ou tables individuels sont déchiffrés en mémoire lors de l'accès. Les données nouvelles ou modifiées sont chiffrées lorsqu'elles sont saisies dans une table et les fichiers journaux d'activité associés (corbeille, rétablir, annuler et erreur) sont également chiffrés.

Le chiffrement de la base de données est transparent pour les utilisateurs, sans perte de fonctionnalité. Lors de l'utilisation de cette fonctionnalité, toutes les instances sont chiffrées, ainsi que le trafic de réplication et les sauvegardes. Le clonage d'instance est toujours disponible avec un impact mineur sur les performances pour l'utilisation du chiffrement de base de données jusqu'à 5 %. Les instances nouvelles et existantes sur les versions prises en charge de peuvent tirer parti du chiffrement de base ServiceNow AI Platform de données.

Comme illustré, ServiceNow stocke et gère les clés à l'aide d'une hiérarchie de clés à trois niveaux :



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Une clé AES-256 spécifique au client est créée par le moteur de base de données et est utilisée pour chiffrer les données.
2. Une deuxième clé AES-256 spécifique au client est créée par le moteur de base de données et est utilisée pour protéger la clé de premier niveau.
3. Une troisième clé AES-256 est créée et stockée dans des dispositifs de gestion de clés validés FIPS 140 dans les centres de ServiceNow données. Cette clé protège la clé de deuxième niveau et est unique pour chaque instance client.

Le prend également en charge le ServiceNow AI Platform cryptage de base de données avec un commutateur fourni par le client, DBE avec CCS. Il s'agit d'une solution de chiffrement qui chiffre toutes les données au repos lorsqu'elles ne sont pas utilisées dans la base de données. Il utilise un cryptage AES standard sans impact sur les fonctionnalités. La base de données chiffre les données telles qu'elles sont écrites sur le disque et déchiffre les données lorsqu'elles sont lues à partir du disque. Cela signifie que les applications disposent toujours des données dans un état non chiffré pour exécuter la logique et les fonctions nécessaires sans impact.

Remarque :
Le chiffrement de base de données n'est pas pris en charge pour les instances sur site.

Si vous utilisez vos propres clés pour le chiffrement de la base de données, reportez-vous à la section Chiffrement de la base de données avec commutateur contrôlé par le client.

Demande de rotation de clé de base de données

Effectuez une rotation annuelle de la clé de base de données ou selon les besoins en soumettant une demande au support.

Avant de commencer

Rôle requis : admin

Important :
À partir de la Washington DC version, Chiffrement de base de données est en cours de préparation pour une dépréciation future. Cloud Encryption est la solution de remplacement du chiffrement des données au repos. Pour plus de détails, voir Chiffrement dans le cloud avec gestion des clés

Pourquoi et quand exécuter cette tâche

La rotation de clés a lieu la nuit dans les 24 heures précédant la date d'expiration et n'interrompt pas le service pour l'instance.

Remarque :
Actuellement, la rotation de clés n'est disponible que dans les ServiceNow environnements commerciaux, GCC (Government Community Cloud), France et Singapour.

Procédure

Contact Service client et assistance pour demander l'une des actions de rotation de clés suivantes :

- Inscrivez-vous pour effectuer une rotation de clés annuelle sur toutes les instances désignées.
- Obtenez un rapport historique des trois dernières rotations clés contenant les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Nom d’instance.
- Nom et version de la clé.
- Dates et heures de rotation.

- Planifiez une rotation de clés anticipée en dehors de la rotation planifiée annuelle.

Chiffrement de la base de données avec commutateur contrôlé par le client

Le chiffrement de la base de données avec commutateur contrôlé par le client (DBE-CCS) est une solution de chiffrement qui chiffre toutes les données au repos lorsqu’elles ne sont pas utilisées dans la base de données.

Important :

Le processus de chiffrement de la base de données avec commutateur contrôlé par le client a commencé son processus de fin de vie et a atteint les étapes de fin de vente et de fin de renouvellement à partir de la version de Yokohama. Pour la prise en charge du chiffrement des données au repos, reportez-vous à la section Chiffrement dans le cloud avec gestion des clés.

Vue d'ensemble

Le chiffrement de la base de données avec commutateur contrôlé par le client utilise le chiffrement AES standard de l’industrie, sans impact sur les fonctionnalités. La base de données chiffre les données telles qu’elles sont écrites sur le disque et déchiffrées par la base de données lorsqu’elles sont lues à partir du disque. Les applications disposent toujours des données dans un état non chiffré pour exécuter la logique et les fonctions nécessaires.

DBE-CCS utilise une technologie native de la base de données, souvent appelée Chiffrement de l’espace de table ou Chiffrement transparent des données. Pour plus de détails sur la technologie, reportez-vous au site Web de MariaDB sous « Tablespace Encryption ».

DBE-CCS vous demande de configurer un point de terminaison de service REST HTTPS qui fournit périodiquement la clé secrète de l’instance ServiceNow . Le point de terminaison CCS renvoie ensuite la clé secrète du client chiffrée avec la clé publique de l’instance de base de données.

Point de terminaison client

Important :

Votre organisation est seule responsable de la configuration et de la maintenance de votre point de terminaison CCS. La spécification du point de terminaison client est fournie dans KB0789788 .

Un ServiceNow partenaire technologique, Fortanix, est disponible pour implémenter votre point de terminaison client pour vous. Contactez directement le partenaire technologique pour plus de détails sur l’intégration. Pour plus d’informations, consultez Utilisation du gestionnaire de sécurité des données Fortanix avec ServiceNow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de ServiceNow plusieurs versions

Important :
Chiffrement de base de données est une offre d'infrastructure payante qui est indépendante de la publication. Elle peut être appliquée à n'importe quelle version prise en charge et à des instances nouvelles ou existantes.

Autres références

Reportez-vous à ces références pour plus d'informations sur le DBE avec CCS :

Référence	Description
KB0993681	Architecture de chiffrement de base de données Commutateur contrôlé par le client
KB0789788	Guide d'implémentation pour DBE avec CCS

Remarque :
Pour accéder aux articles de la base de connaissances, vous devez d'abord vous authentifier dans Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des accès

La gestion des accès vous permet d'accéder à l'instance ServiceNow® en toute sécurité.

Accès zéro confiance



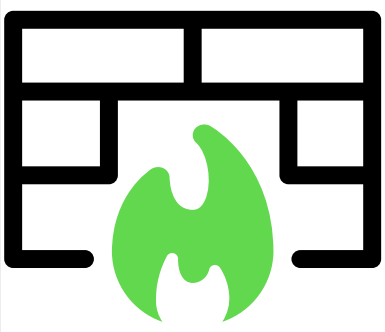
L'accès Zero Trust garantit que tous les accès aux applications et aux données sont accordés sur la base d'un moindre privilège, uniquement après la vérification de l'identité de l'utilisateur et l'évaluation des risques.

Séparation en domaines



Grâce à , les fournisseurs de services (SP) peuvent fournir à leurs clients une intégration plus rapide, respecter la conformité et protéger leurs données à l'aide de ServiceNow AI Platform Séparation de domaine.

Authentification

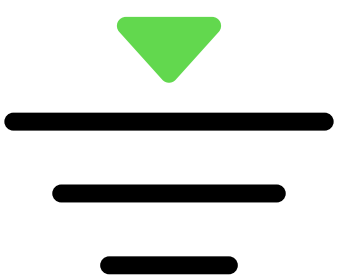


L'authentification de ServiceNow valide l'identité d'un utilisateur qui accède à une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de poste de l'utilisateur.

ACL



Filtration des données



Rôles de sécurité



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

Les rôles de sécurité offrent une sécurité supplémentaire. Chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse distinguer les utilisateurs internes des utilisateurs externes.

Connexions et informations d'identification



Les informations d'identification et de connexion sont nécessaires pour accéder à un ordinateur ou à un appareil réseau pour Découverte, Mappage des services et Gestion cloud, ou pour travailler avec Orchestration.

Contrôle d'accès ServiceNow



Le module d'extension Contrôle d'accès SNC vous permet de contrôler quels employés du service clientèle et de l'assistance peuvent accéder à votre instance, et quand.

Accès zéro confiance (ZTA)

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’accès Zero Trust.

Activer



Découvrez comment activer l’accès Zero Trust.

Configurer



Configurer l’accès zéro confiance.

Référence : Propriétés



Renseignez-vous sur les propriétés de l’accès Zero Trust.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l'accès zéro confiance

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

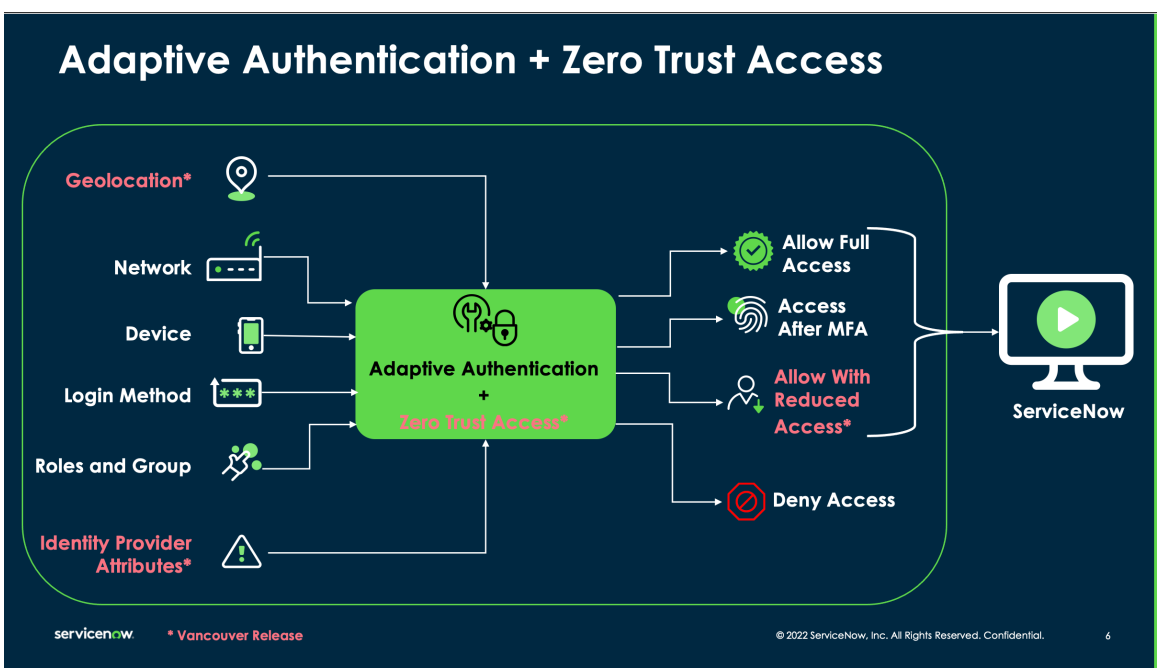
ZTA garantit que tous les accès aux applications et aux données sont accordés sur la base d'un moindre privilège, uniquement après la vérification de l'identité de l'utilisateur et l'évaluation des risques.

Zero Trust - Accès à la session basé sur des politiques

ServiceNow Zero Trust - Accès à la session basé sur des politiques (Session Access) permet aux organisations de réduire dynamiquement les privilèges de l'utilisateur dans une session Web en fonction de divers facteurs, notamment l'adresse IP, l'emplacement, la méthode d'authentification, le rôle de l'utilisateur, le groupe, l'utilisateur disposant d'une MFA et les attributs partagés par le fournisseur d'identité (IdP). Cela peut aider à protéger les organisations contre les accès non autorisés et les violations de données, même lorsque les utilisateurs avec des privilèges élevés accèdent aux applications à partir d'appareils ou d'emplacements non approuvés.

Zero Trust - Accès à la session basé sur des politiques

Elle permet aux administrateurs de sécurité de réduire ou de limiter l'accès des utilisateurs dans une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement à la session connectée. L'utilisateur continue d'accéder à l'instance avec les privilèges affectés.
- L'accès à la session n'a aucun impact tant que l'utilisateur est déjà connecté à l'instance et que l'administrateur configure simultanément la politique. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session n'a aucun impact lorsque l'utilisateur se trouve dans un réseau de confiance et passe ensuite à un VPN (changement d'emplacement ou de réseau) au cours d'une session.
- L'accès à la session est appliqué au moment de la connexion. Tout changement apporté aux paramètres de risque pendant la session n'entraînera pas de réduction de l'accès. Par exemple, le passage d'un utilisateur du réseau d'entreprise à un réseau non approuvé après l'établissement de la session n'entraînera pas de réduction de l'accès, sauf s'il se déconnecte et se reconnecte.
- Session Access (Zero Trust Access - ZTA), les rôles tels que snc_internal et snc_external ne peuvent pas être supprimés.
- La fonctionnalité d'accès à la session (Accès zéro confiance : ZTA) ne supprime pas un rôle de la table d'appartenance au sys_user_has_role ou au groupe d'utilisateurs. Basé sur la politique ZTA, il établit la session utilisateur avec des rôles réduits ou limités.
- Les scripts exécutés dans le contexte du système ne respecteront pas les rôles de session ZTA.

Cas d'utilisation

Voici quelques-uns des cas d'utilisation de l'accès Zero Trust :

- Réduisez les privilèges en fonction du risque associé à la session. Par exemple, un utilisateur avec le rôle de prestataire qui se connecte depuis l'extérieur du réseau approuvé peut être configuré pour n'avoir que le rôle de demandeur pour la session.
- Réduisez l'accès en fonction de la réponse IdP pour une session utilisateur, si l'utilisateur utilise un appareil non approuvé. Pour plus d'informations, consultez Configurer l'attribut de fournisseur d'identité pour l'accès à la session.

Cette relégation de rôle garantit que l'utilisateur ne dispose d'aucun autre privilège existant dans une session. Lorsque l'utilisateur se connecte à partir d'un réseau de confiance, tous les privilèges existants sont affectés pour une session.

Plusieurs conditions d'adresses IP et plusieurs affectations de rôles ou de groupes peuvent être définies dans le cadre de la politique.

Accès zéro confiance : mobile

Vous pouvez utiliser la stratégie Accès zéro confiance - Accès à la session dans le cadre de la politique d'authentification adaptative pour réduire les rôles ou les privilèges d'une session spécifique sur mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accès zéro confiance : Accès à la session mobile peut être activé en activant **glide.authenticate.session_access.mobile.enabled** dans la table des propriétés système.

Pour utiliser l'accès zéro confiance : Session Access mobile avec les attributs IdP, vous pouvez configurer le champ **glide.authenticate.session_access.mobile.refresh_token_interval** . Cela permet aux administrateurs de contrôler efficacement l'accès à la session en fonction du jeton d'actualisation.

Pour plus d'informations, consultez Configure Zero Trust Access for mobile .

Activation de l'accès zéro confiance

Activez le module d'extension **Zero Trust - Policy Based Session Access** com.snc.zero_trust_session_access pour permettre aux administrateurs de sécurité de réduire ou de limiter l'accès des utilisateurs dans une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.

Avant de commencer

Rôle requis : admin

Type de module d'extension : payant et nécessitant une licence.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension **Zero Trust - Policy Based Session Access** (com.snc.zero_trust_session_access) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Configuration du rôle d'accès à la session

Configurez l'accès à la session pour réduire l'accès des utilisateurs dans une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.

Avant de commencer

Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement à la session connectée. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui sont affectés.
- L'accès à la session n'a aucun impact tant que l'utilisateur est déjà connecté à l'instance et que l'administrateur configure simultanément la politique. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session est appliqué au moment de la connexion. Tout changement apporté aux paramètres de risque pendant la session n'entraînera pas de réduction de l'accès. Par exemple, un utilisateur passant du réseau d'entreprise à un réseau non approuvé après avoir établi la session n'entraînera pas de réduction de l'accès à moins que l'utilisateur ne se déconnecte et ne se reconnecte.
- Session Access (Zero Trust Access - ZTA), les rôles tels que snc_internal et snc_external ne peuvent pas être supprimés.
- La fonctionnalité d'accès à la session (Accès zéro confiance : ZTA) ne supprime pas un rôle de la table d'appartenance au sys_user_has_role ou au groupe d'utilisateurs. Basé sur la politique ZTA, il établit la session utilisateur avec des rôles réduits ou limités.
- Les scripts exécutés dans le contexte du système ne respecteront pas les rôles de session ZTA.

Procédure

1. Accédez à la **Tous** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.
2. Pour créer une configuration de rôle d'accès à la session, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire :

Configuration du rôle d'accès à la session

Champ	Description
Nom	Nom de la configuration
Description	Brève description de la configuration.
Politique	Choisissez la politique d'authentification adaptative. Utilisez l'icône de recherche pour afficher la liste des politiques.
Action	**Supprimez les rôles** ou **limitez-les aux rôles**. ○ **Supprimer les rôles** : lorsque l'utilisateur configuré se connecte, la liste des rôles fournie dans la liste de rôles ou de groupes est supprimée pour la session. ○ **Limiter aux rôles** : lorsque l'utilisateur configuré se connecte, seuls les rôles

Traduction automatique

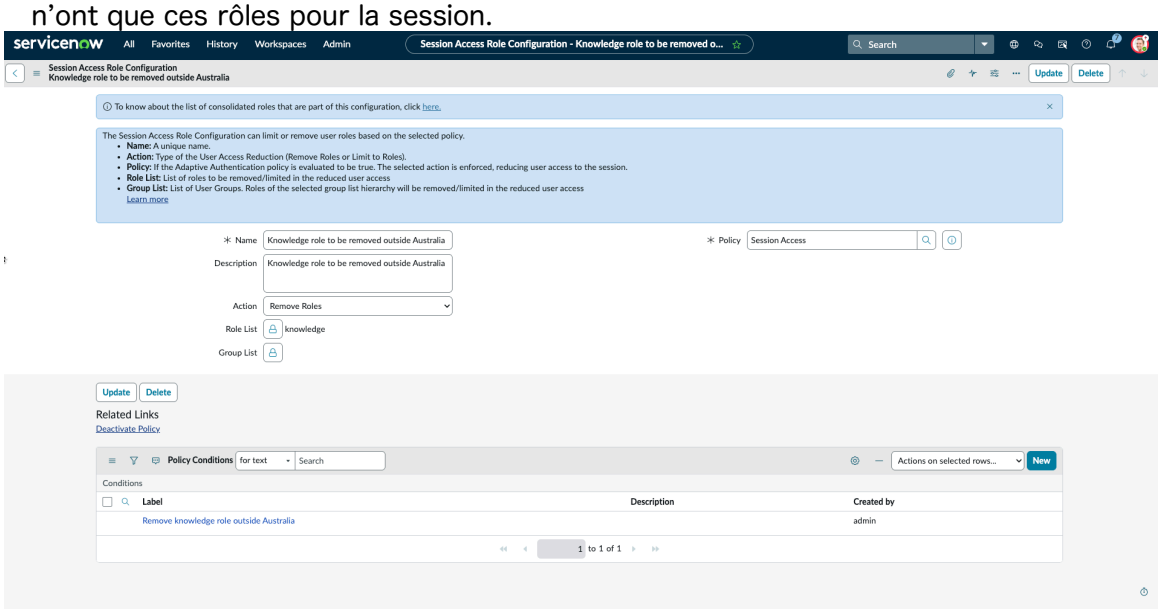
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	sélectionnés sont fournis à l'utilisateur et tous les autres rôles sont supprimés pour la session.
Liste de rôles	Choisissez des rôles dans la liste de rôles.
Liste de groupes	Choisissez les rôles dans la liste de groupes que vous souhaitez supprimer ou limiter à l'utilisateur.

4. Sélectionner, **soumettre**.

   La connexion pour les utilisateurs en fonction des pays configurés est la suivante :

   - Dans **Supprimer les rôles**, les utilisateurs des pays configurés avec les rôles sélectionnés n'ont plus ces rôles pour la session.
   - Dans **Limiter aux rôles**, les utilisateurs des pays configurés avec les rôles sélectionnés n'ont que ces rôles pour la session.



   Pour en savoir plus sur la suppression ou la limitation des rôles d'une session expliquée à l'aide d'un exemple de cas d'utilisation, reportez-vous à la section Didacticiel : Utiliser l'accès zéro confiance.

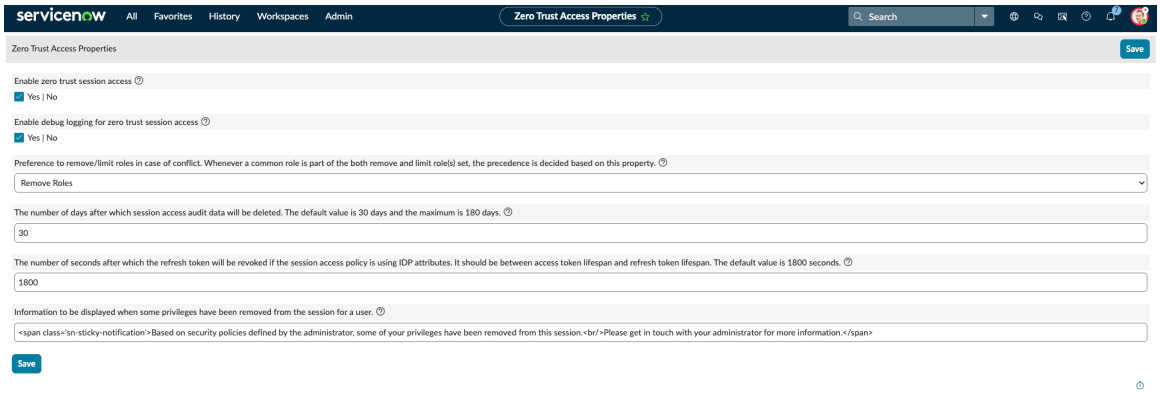
Propriétés système de l'accès Zero Trust

Utilisez les propriétés système pour activer et personnaliser l'accès Zero Trust afin de répondre à vos exigences de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés



Propriétés système de l'accès Zero Trust

Propriété	Description
Activer l'accès Zero Trust à la session	Option qui permet aux administrateurs d'utiliser la fonctionnalité d'accès à la session Zero Trust. Par défaut, la valeur est faux.
Activer la journalisation de débogage pour l'accès à la session Zero Trust	Option permettant d'activer la journalisation de débogage pour l'accès à la session Zero Trust.
Préférence pour supprimer/limiter les rôles en cas de conflit. Lorsqu'un rôle commun fait partie à la fois des rôles de suppression et de limite définis, la priorité est définie en fonction de cette propriété.	**Supprimer les rôles** ou **limiter les rôles**
Nombre de jours après lesquels les données d'audit d'accès à la session sont supprimées. La valeur par défaut est de 30 jours et la valeur maximale de 180 jours.	Par défaut, il est de 30 jours.
Nombre de secondes après lesquelles le jeton d'actualisation est révoqué si la politique d'accès à la session utilise des attributs IdP. Il doit être compris entre la durée de vie du jeton d'accès et la durée de vie du jeton d'actualisation. La valeur par défaut est de 1 800 secondes.	Par défaut, il est de 1800 secondes.
Informations à afficher lorsque certains privilèges ont été supprimés de la session pour un utilisateur.	Description que vous souhaitez afficher à vos utilisateurs concernant la limitation ou la suppression de privilèges. Description de l'échantillon : En fonction des politiques de sécurité définies par l'administrateur, certains de vos rôles ont été supprimés de cette session. Contactez votre administrateur pour plus d'informations.

Audits d'accès à la session

Les audits d'accès à la session affichent les journaux d'accès à la session et les informations relatives à la session d'un utilisateur.

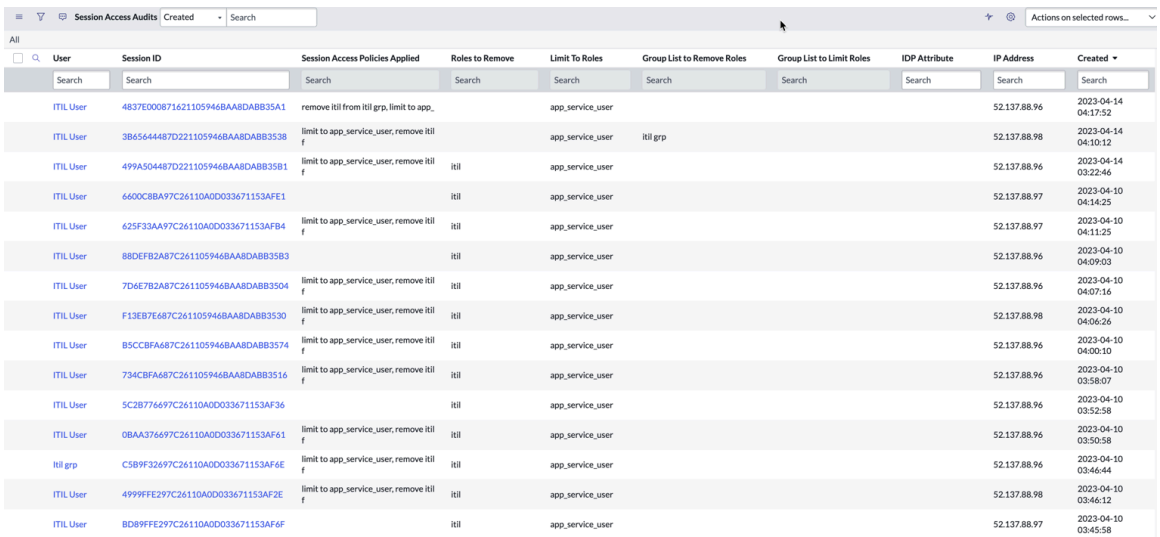
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Audits

L'audit d'accès à la session affiche les informations d'audit comme suit :

Remarque :
Utilisez la propriété glide.authenticate.session_access.log_audit_event pour renseigner les informations d'audit.



Audits d'accès à la session

Champ	Description
Utilisateur	Détails de l'utilisateur.
ID de session	Les détails de la session sont affichés sous la forme d'un ID unique.
Client mobile	Détails du client mobile. **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now Mobile).
Politiques d'accès à la session appliquées	La politique d'accès à la session appliquée.
Rôles à supprimer	Rôles qui ont été supprimés de l'utilisateur lors de la connexion.
Limiter aux rôles	Rôles qui ont été limités à l'utilisateur lors de la connexion.
Liste de groupes pour supprimer les rôles	Informations sur le groupe qui a supprimé les rôles de l'utilisateur.
Liste de groupes pour limiter les rôles	Informations sur le groupe qui a des rôles limités pour l'utilisateur.
Client mobile	Détails de l'utilisateur connecté via un mobile avec un accès réduit ou supprimé.
Attribut IdP	L'IDP qui a été utilisé pour cette session.
Adresse IP	Détails de l'adresse IP utilisée par l'utilisateur pour se connecter.
Créées	Détails de la date et de l'heure de création de l'enregistrement utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Didacticiel : Utiliser l'accès zéro confiance

Procédure d'utilisation de la fonctionnalité d'accès zéro confiance avec un cas d'utilisation de bout en bout.

Avant de commencer
Rôle requis : security_admin

Activez la **propriété Activer l'accès à la session**.

Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement à la session connectée. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui sont affectés.
- L'accès à la session n'a aucun impact tant que l'utilisateur est déjà connecté à l'instance et que l'administrateur configure simultanément la politique. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session est appliqué au moment de la connexion. Tout changement apporté aux paramètres de risque pendant la session n'entraînera pas de réduction de l'accès. Par exemple, un utilisateur passant du réseau d'entreprise à un réseau non approuvé après avoir établi la session n'entraînera pas de réduction de l'accès à moins que l'utilisateur ne se déconnecte et ne se reconnecte.
- Session Access (Zero Trust Access - ZTA), les rôles tels que snc_internal et snc_external ne peuvent pas être supprimés.
- La fonctionnalité d'accès à la session (Accès zéro confiance : ZTA) ne supprime pas un rôle de la table d'appartenance au sys_user_has_role ou au groupe d'utilisateurs. Basé sur la politique ZTA, il établit la session utilisateur avec des rôles réduits ou limités.
- Les scripts exécutés dans le contexte du système ne respecteront pas les rôles de session ZTA.

L'accès à la session est une fonctionnalité qui permet aux administrateurs de réduire ou de restreindre dynamiquement un ensemble de rôles à l'utilisateur, lorsque celui-ci tente de se connecter à l'instance à partir de différents environnements, par exemple à partir d'un réseau non approuvé, d'un appareil différent, etc.

L'accès à la session peut être contrôlé par la politique créée et l'action sélectionnée lors de l'exécution de la configuration. Voici quelques-uns des scénarios :

- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Supprimer les rôles**, les rôles sélectionnés et ses rôles enfants associés sont supprimés pour l'utilisateur lors de la tentative de connexion à l'instance.
- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Limiter aux rôles**, seuls les rôles sélectionnés et ses rôles enfants associés sont affectés à l'utilisateur lors de la tentative de connexion à l'instance.

La procédure suivante explique une configuration de bout en bout de la configuration d'accès à la session en fonction de laquelle le rôle est limité à l'utilisateur qui se connecte à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'instance. De même, vous pouvez également supprimer des rôles en sélectionnant l'option **Supprimer les rôles** pendant la configuration.

Procédure

1. Accédez à la **Tous** > **Accès à la session** > **Configurations du rôle d'accès à la session**.
2. Sur la page Configuration des rôles d'accès à la session, sélectionnez **Nouveau**.
3. Pour limiter un rôle pour l'utilisateur, renseignez les champs du formulaire :
   - Nom
   - Description
   - Politique
   - Action
   - Liste de rôles
   - Liste de groupes

   a. Choisissez **Limiter aux rôles** pour limiter les rôles de l'utilisateur. Par exemple, **itil**.

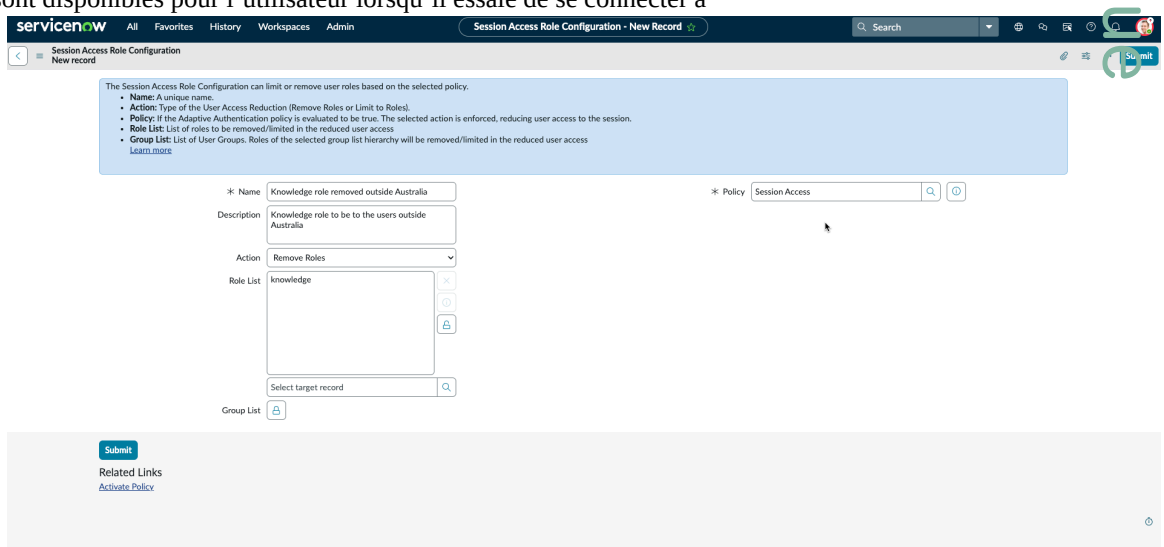
   b. Choisissez le rôle de **la base de connaissances** dans la liste des rôles.

   c. Choisissez la **politique**.

   Vous pouvez créer la politique d'accès à la session à l'aide de politiques d'authentification et de critères de filtre (rôle, groupe, adresse IP, emplacement) avec des entrées et des conditions de politique.

   Utilisez la politique dans la configuration de l'accès à la session. Par exemple, vous souhaitez limiter le rôle (connaissances) à l'utilisateur qui se connecte en dehors de l'emplacement (Australie).

   d. Choisissez Action comme **limite aux rôles**. Si la politique est vraie, seuls les rôles sélectionnés et leurs rôles enfants associés sont disponibles pour l'utilisateur lorsqu'il essaie de se connecter à l'instance.



Traduction automatique

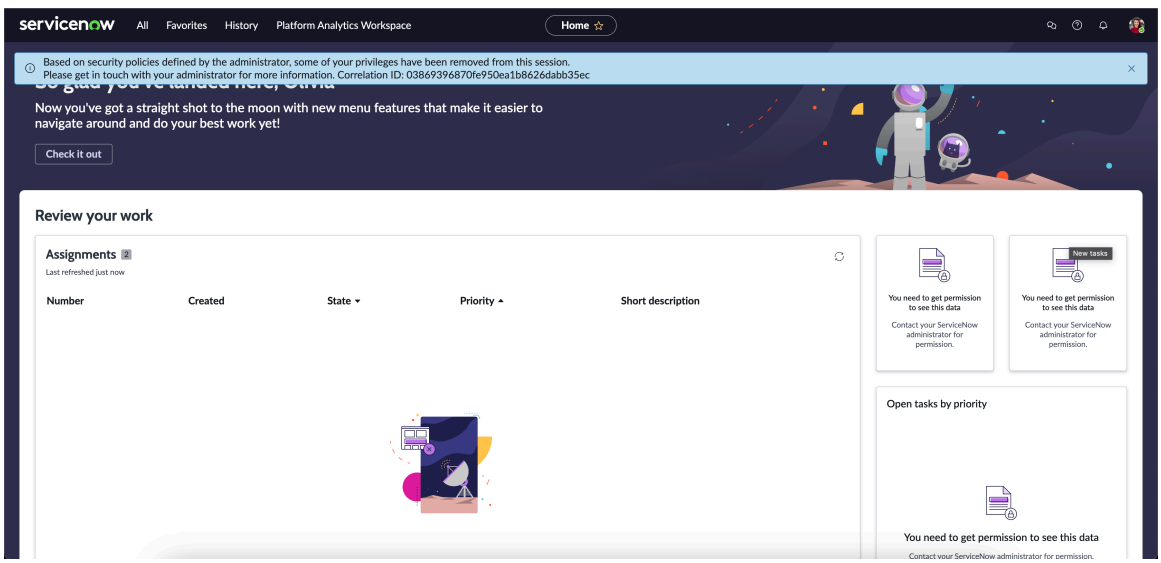
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Sélectionnez **Soumettre**.

De même, vous pouvez choisir le groupe dans la liste des groupes pour restreindre ou supprimer des rôles pour les utilisateurs au sein du groupe.

Lorsque l'utilisateur se connecte à l'instance en dehors de l'Australie, seul le rôle **Connaissances** et ses rôles enfants associés sont affectés pour la session connectée, et les autres rôles de l'utilisateur sont limités.

Après s'être connecté, l'utilisateur s'affiche avec le message d'erreur suivant sur la plateforme dans sa section de profil :



L'utilisateur peut contacter les administrateurs et fournir l'ID de corrélation pour l'enquête.

Remarque :
L'ID de corrélation est le sys_id de l'enregistrement d'audit correspondant dans la table d'audit d'accès à la session.

Configurer l'attribut de fournisseur d'identité pour l'accès à la session

Utilisez l'attribut Fournisseur d'identité (IdP) créé à partir de la réponse SAML (Security Assertion Markup Language) et OpenID Connect (OIDC) pour supprimer ou restreindre l'accès de session utilisateur à l'instance.

Avant de commencer

Rôle requis : security_admin

Activez la **propriété Activer l'accès à la session**.

Remarque :
Pour utiliser la configuration du rôle d'accès à la session, vous devez élever votre rôle à `security_admin`.

L'accès à la session peut être contrôlé par la politique créée et l'action sélectionnée lors de l'exécution de la configuration. Voici quelques-uns des scénarios :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Supprimer les rôles** ainsi que l'entrée et la condition d'attribut IdP, les rôles sélectionnés et leurs rôles enfants associés sont supprimés pour l'utilisateur lors de la tentative de connexion à l'instance.
- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Limiter aux rôles** avec l'entrée et la condition de l'attribut IdP, seuls les rôles sélectionnés et ses rôles enfants associés sont affectés à l'utilisateur lors de la tentative de connexion à l'instance.

La procédure suivante montre les étapes de configuration de l'attribut IdP à partir de la réponse SAML, une entrée de politique pour contrôler l'accès à la session.

Procédure

1. Accédez à la **Tous** > **Accès à la session** > **Configurations du rôle d'accès à la session**.
2. Sur la page Configuration des rôles d'accès à la session, sélectionnez **Nouveau**.
3. Pour supprimer tout rôle de l'utilisateur, renseignez les champs suivants du formulaire :
   - Nom
   - Description
   - Politique
   - Action
   - Liste de rôles
   - Liste de groupes

   a. Choisissez **Supprimer les rôles** pour supprimer les rôles de l'utilisateur.
   Par exemple : **itil**.

   b. Choisissez le rôle **itil** dans la liste des rôles.

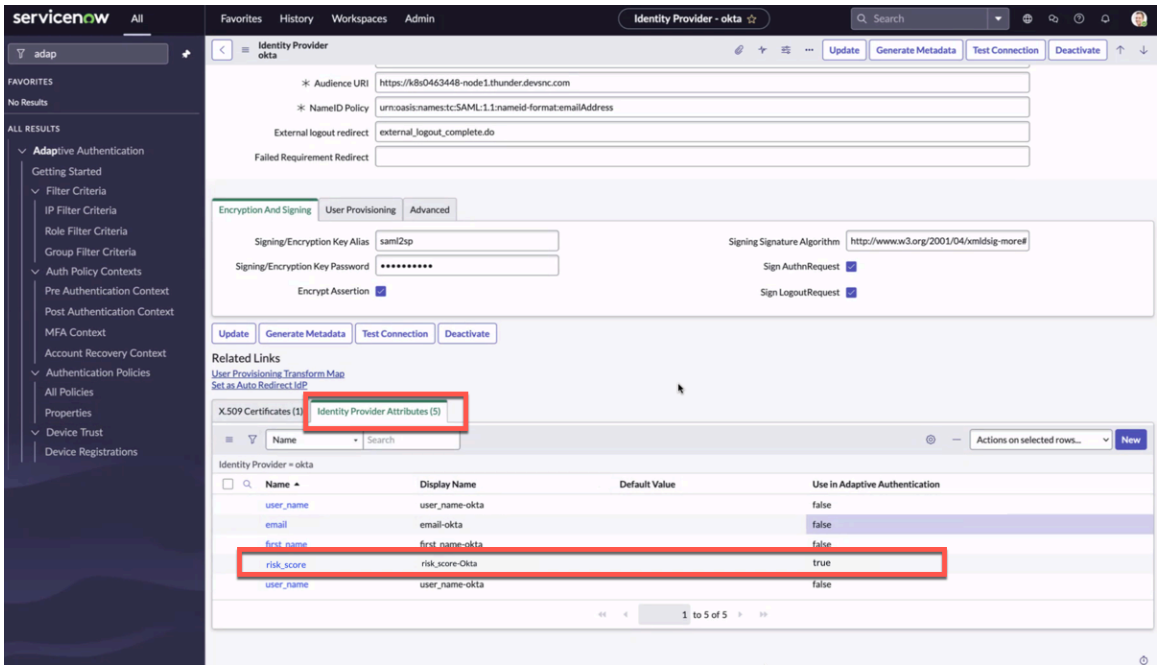
   c. Choisissez la **politique**.
   Pour en savoir plus sur la création d'une stratégie à l'aide de différents critères de filtre à l'aide de la création de stratégie d'authentification adaptative, reportez-vous à la section Critère de filtre.

   d. Choisissez Action comme rôles de suppression.
   Si la politique est définie sur vrai et que l'action sur les rôles est définie sur **Supprimer les rôles**, les rôles sélectionnés sont supprimés pour l'utilisateur lors de la tentative de connexion à l'instance.

   e. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.
   Par exemple :
   - **Entrée de politique** : attribut de score de risque d'Okta (IDP).
   - **Conditions de la politique** : Score de risque de 60 à 80 comme condition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Selon cette configuration, lorsque la valeur de l'attribut de score de risque d'Okta (IdP) dépasse 80, l'utilisateur n'est pas authentifié avec les rôles (**employé**) et ses rôles enfants qui ont été supprimés de l'instance, l'utilisateur est authentifié uniquement avec d'autres rôles affectés. Si le score de risque est compris entre 60 et 80, l'utilisateur est authentifié auprès de l'instance avec tous les rôles.

Pour plus d'informations sur la création d'une politique de contexte de post-authentification avec des entrées et une condition de politique, reportez-vous à la section Contexte de post-authentification.

Remarque :
Si la propriété **Activer l'accès** à la session est inactive, la configuration de l'accès à la session ne restreint ni ne supprime les rôles de l'utilisateur.

f. Sélectionnez **Soumettre**.

Accès zéro confiance pour mobile

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

Vous pouvez utiliser la stratégie Accès zéro confiance - Accès à la session dans le cadre de la politique d'authentification adaptative pour réduire les rôles ou les privilèges d'une session spécifique dans Mobile pour les utilisateurs.

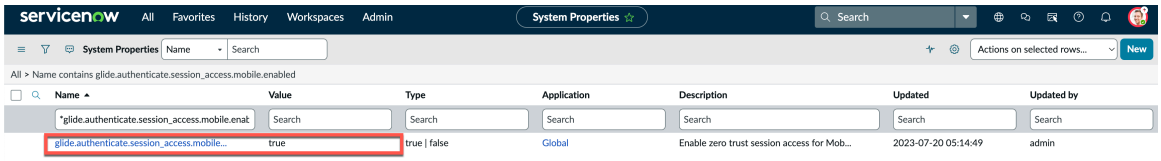
Pour activer l'accès zéro confiance sur mobile, vous devez effectuer les tâches suivantes :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- Activez la politique de com.snc.zero_trust_session_access**Zero Trust - Accès à la session basé sur des politiques**.

Traduction automatique

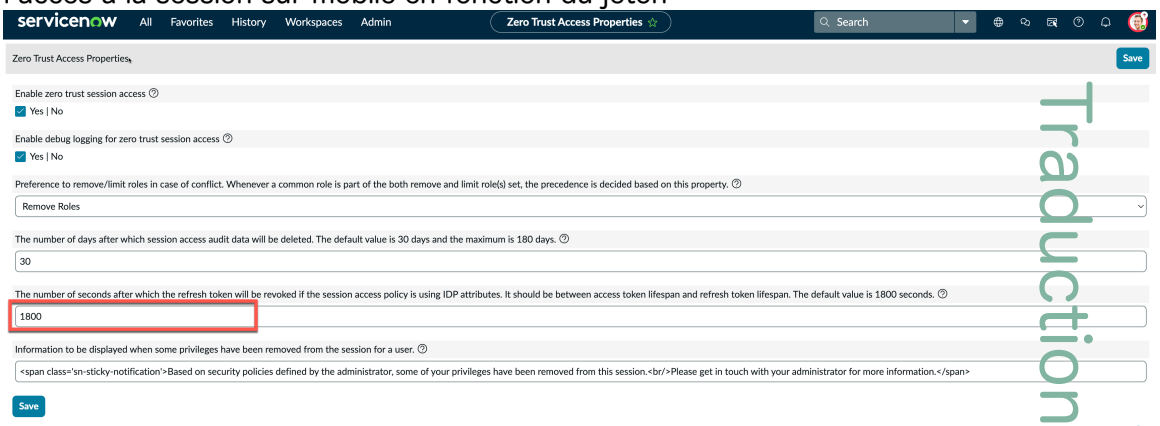
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez **l'option glide.authenticate.session_access.mobile.enabled** à partir de la table des propriétés



système.

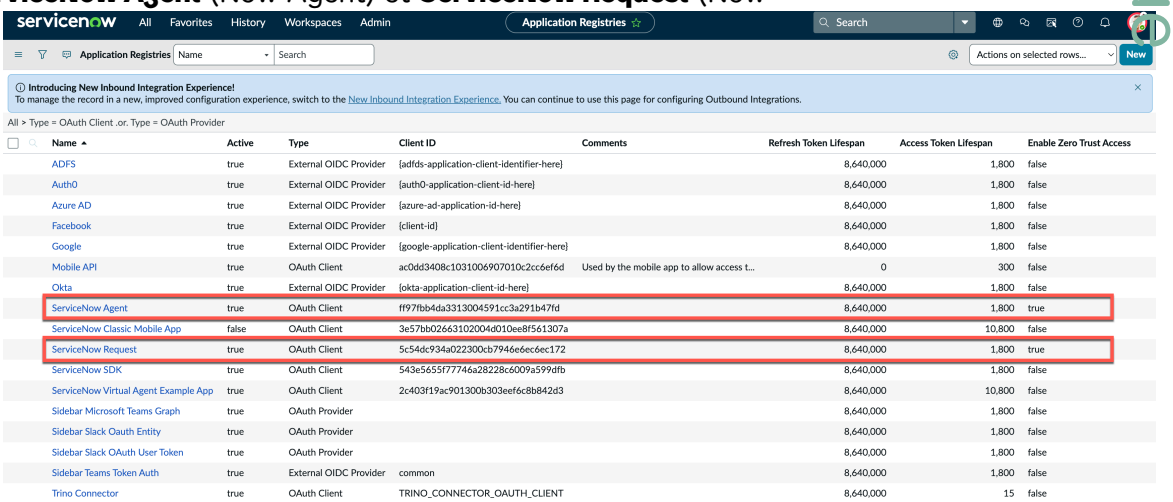
- Configurez le champ **glide.authenticate.session_access.mobile.refresh_token_interval** pour contrôler l'accès à la session sur mobile en fonction du jeton



d'actualisation.

> **Remarque :**
> Vous devez configurer les secondes du jeton d'actualisation lors de l'utilisation d'un IDP pour les connexions à l'application mobile. Par défaut, les utilisateurs sont déconnectés des applications mobiles après 1 800 secondes (30 minutes).

- Définissez Activer l'accès zéro confiance sur vrai sous **Registres d'application** pour l'application cliente mobile (client OAuth). Dans ce cas, **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now



Mobile).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurez le rôle d’accès à la session pour réduire ou supprimer les rôles des utilisateurs qui se connectent en fonction des entrées et des conditions de la politique. Pour en savoir plus sur la configuration, reportez-vous à la section Configuration du rôle d’accès à la session.

La configuration évalue la connexion pour réduire ou supprimer les rôles des utilisateurs qui accèdent à votre ServiceNow® instance en fonction des filtres et conditions de politique. Pour plus d'informations, consultez Configure Zero Trust Access for mobile .

Authentification continue (CA)

ServiceNow L’authentification continue de vous permet de revérifier et d’authentifier un utilisateur s’il accède à des ressources que vous protégez.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’authentification continue.

Activer



Découvrez comment activer l’authentification continue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Configurez l’authentification continue.

Référence : Propriétés



Connaître les propriétés de l’authentification continue.

Explorer l’authentification continue

ServiceNow L’authentification continue de vous permet de revérifier et d’authentifier un utilisateur s’il accède à des ressources que vous protégez.

ServiceNow est un mécanisme de sécurité conçu pour vérifier l’identité d’un utilisateur non seulement lors de la connexion initiale, mais tout au long de la session de l’utilisateur. CA repose sur ServiceNow l’architecture de sécurité d’accès Zero Trust de qui vise à améliorer la sécurité en veillant à ce que l’utilisateur reste celui qu’il prétend être, même après le processus d’authentification initial.

CA fonctionne sur les principes d’accès Zero Trust suivants :

- **Vérifier explicitement** : aucune confiance implicite pour un utilisateur, un appareil ou un système au sein d’un réseau, quel que soit son emplacement. Chaque utilisateur et appareil doit être explicitement authentifié et autorisé, quel que soit l’emplacement ou l’accès passé.
- **Utilisez l’accès avec le moins de privilèges** : n’accordez que l’accès ou les autorisations minimales nécessaires pour effectuer des tâches spécifiques et limiter les dommages potentiels causés par des comptes ou des systèmes compromis.
- **Supposer une violation** : au lieu de vous fier uniquement à la prévention, supposez une violation et concentrez-vous sur la détection, le confinement et la réponse proactifs.

CA offre la possibilité d’appliquer une authentification renforcée ou une nouvelle authentification en fonction des données auxquelles les utilisateurs accèdent et des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

activités qu'ils effectuent. Il peut être choisi par les administrateurs pour créer des politiques de sécurité au niveau d'une table ou d'une classe de données.

Vous pouvez appliquer une authentification renforcée (MFA) ou une nouvelle authentification (SSO : SAML ou OIDC) au sein d'une session connectée chaque fois que l'utilisateur tente d'accéder à des informations personnelles identifiables (PII) et à des données sensibles.

Remarque :
Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.

Avantages

Voici quelques-uns des avantages de l'utilisation de l'autorité de certification :

- **Sécurité renforcée** : en vérifiant continuellement l'identité de l'utilisateur, le système peut détecter et répondre plus rapidement aux menaces de sécurité potentielles.
- **Réduction du risque de prise de contrôle de compte** : même si un attaquant accède à la session d'un utilisateur, l'authentification continue peut l'empêcher d'accéder à des données confidentielles.

Cas d'utilisation

Voici quelques-uns des cas d'utilisation de l'autorité de certification :

- Appliquez une nouvelle authentification avant d'autoriser l'accès à des données sensibles à l'aide de politiques différentes.
- Appliquez une nouvelle authentification périodique ou une authentification renforcée à l'aide de différentes politiques :
  - Utilisez une nouvelle authentification qui peut inclure la MFA d'IdP, l'authentification unique d'IdP.
  - Utilisez l'authentification avancée avec ServiceNow la MFA de .

Rôles dans CA

Le CA a les rôles suivants :

- Administrateur CA (ca_admin) : capacité à créer, modifier et afficher les politiques CA. Configurez les propriétés CA et affichez les tableaux de bord (mesures) de CA.
- Administrateur de politique (ca_policy_admin) : capacité à créer, modifier et afficher les politiques de l'autorité de certification.
- Auditeur (ca_auditor) : capacité à afficher les tableaux de bord (mesures) de CA. Et les politiques, et les journaux de CA.

Pour configurer CA, vous devez élever votre rôle à **ca_admin** et effectuer les configurations de politique.

Remarque :
Ces 3 rôles sont tous des rôles élevés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules dans CA

Les différents modules de CA sont les suivants :

- Politiques : affichez les différentes politiques d'authentification continue créées.
- Mesures : affichez les différentes mesures pour l'authentification continue à des fins de KPI et comprenez l'utilisation de l'autorité de certification au sein de votre organisation.
- Propriétés système : utilisez les propriétés système pour activer et personnaliser l'authentification continue (CA) afin de répondre à vos exigences de sécurité d'accès Zero Trust.

Information associée

Politiques

Mesures

Propriétés système

Travail préalable pour l'authentification continue

Activation de l'authentification continue

Configuration de l'authentification continue

Session d'assurance élevée avec authentification continue

Politiques

Affichez les différentes politiques d'authentification continue créées.

Le formulaire Politiques de CA inclut les détails des politiques de CA créées pour la table ou la classe de données. Vous pouvez gérer les enregistrements de politique à partir des politiques personnalisées.

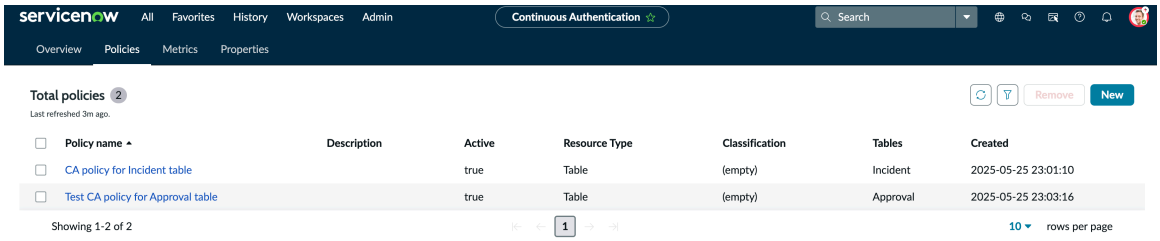
Pour accéder à la page des politiques, accédez à **Tous** > **Authentification continue**, sélectionnez l'onglet **Politiques** . Les détails de la politique affichés sur la page sont les suivants :

Page Politiques

Champ	Description
Nom de la politique	Nom de la politique
Description	Description de la politique
Actif	État de la politique
Type de ressource	Type de ressource sélectionné utilisé pour la politique
Classification	Classification des données sélectionnée pour la politique
Tables	Tables sélectionnées pour la politique
Créées	Détails de création de politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Information associée

- Mesures
- Propriétés système
- Explorer l’authentification continue

Mesures

Affichez les différentes mesures d’authentification continue.

Pour accéder à la page des mesures, accédez à **Tous** > **Authentification continue**, sélectionnez l’onglet **Mesures** .

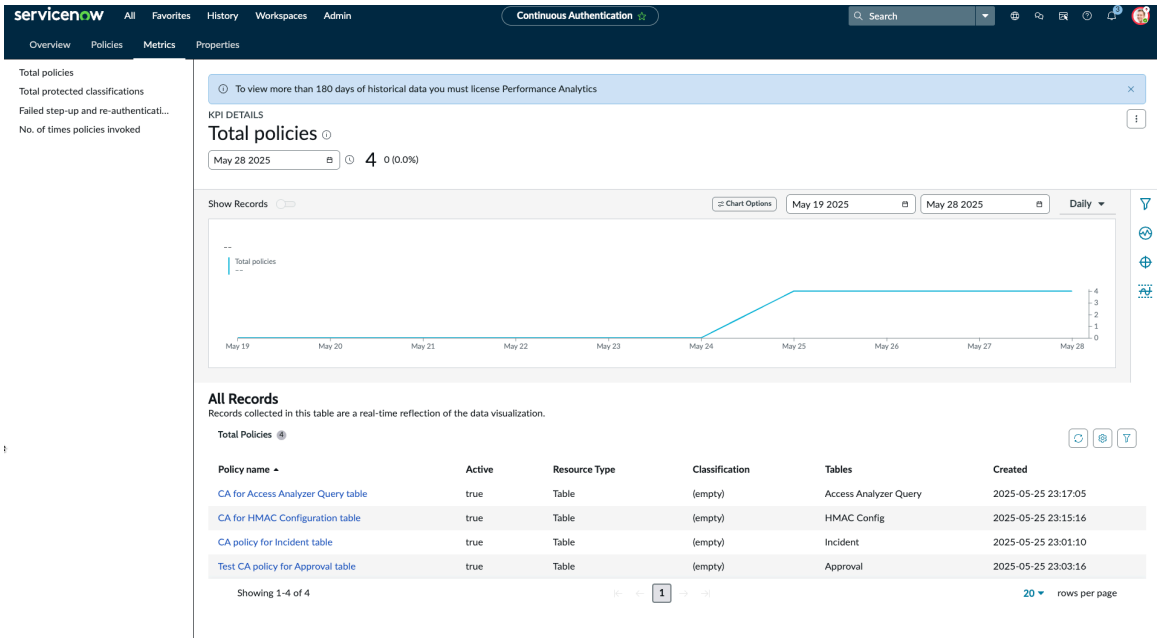
Voici les différents détails des KPI que vous pouvez afficher pour l’authentification continue :

Mesures

Mesures	Description
Politiques totales	KPI pour le nombre de politiques d’authentification continue créées pour les utilisateurs.
Classifications protégées totales	KPI pour le nombre de classifications protégées en raison de la création de la politique CA.
Échec de l’escalade ou de la nouvelle authentification	KPI pour le nombre d’échecs d’escalade (MFA) ou de réauthentification (SSO).
Nombre de fois où les politiques sont appelées	KPI pour le nombre total d’appels des politiques CA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Les détails des KPI sont affichés pendant 180 jours. Pour afficher plus de 180 jours de données historiques, vous devez posséder une licence **Analyse des performances**.

Information associée

- Politiques
- Mesures
- Propriétés système
- Explorer l’authentification continue

Propriétés système

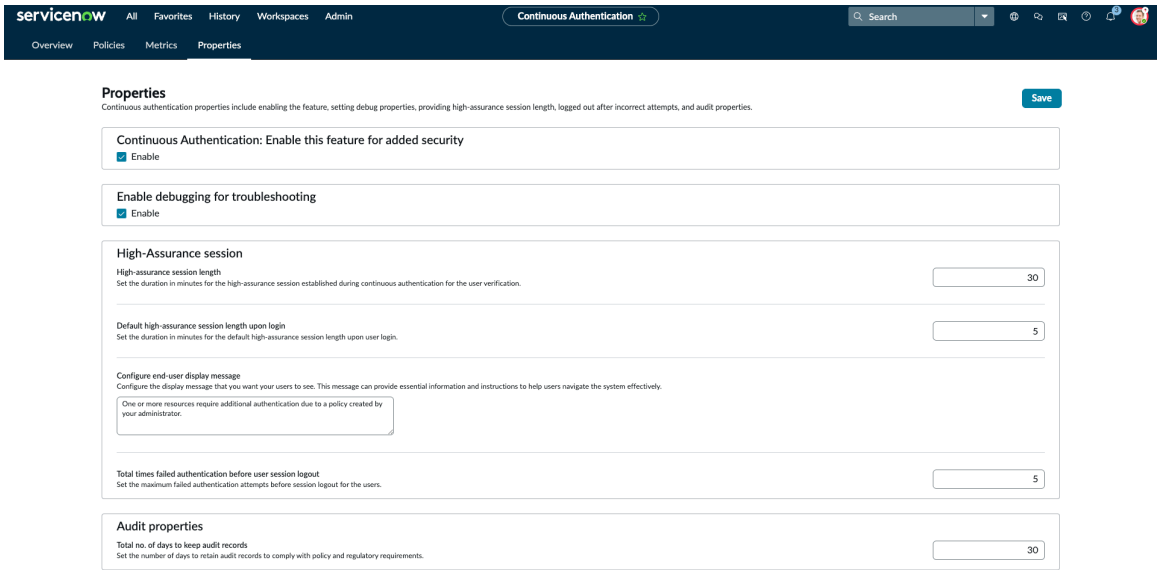
Utilisez les propriétés système pour activer et personnaliser l’authentification continue (CA) afin de répondre à vos exigences de sécurité d’accès Zero Trust.

Propriétés

Pour accéder à la page des propriétés, accédez à **Tous** > **Authentification continue**, sélectionnez l’onglet **Propriétés** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les différentes propriétés système pour l'autorité de certification sont les suivantes :

Propriétés système de l'authentification continue

Propriété	Description
Propriétés générales	
Authentification continue (*glide.zta.continuous_authentication.enabled*)	Activer pour utiliser la fonctionnalité d'authentification continue
Activer le débogage (*glide.zta.continuous_authentication.debug.enabled*)	Activez cette option pour afficher les informations de débogage dans l'authentification continue.
Assurance élevée	
Durée de la session d'assurance élevée (*glide.zta.high_assurance.session.timeout*)	Spécifiez la durée de la session d'assurance élevée, après laquelle les utilisateurs finaux doivent s'authentifier à nouveau. Par défaut : 10 minutes. **Remarque :** La valeur doit être comprise entre 1 et 480.
Durée de session d'assurance élevée par défaut lors de la connexion (*glide.zta.default.high_assurance.session.timeout*)	Spécifiez la durée en minutes de la durée de session à assurance élevée par défaut à compter de la connexion de l'utilisateur. Valeur par défaut : **5** minutes. **Remarque :** La propriété est uniquement applicable pour la connexion locale.
Configurer le message d'affichage de l'utilisateur final (*glide.zta.high_assurance.session.message*)	Spécifiez le message qui s'affiche à l'utilisateur final pour une nouvelle authentification. Message par défaut : une ou plusieurs ressources nécessitent une authentification supplémentaire en raison d'une politique créée par votre administrateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système de l'authentification continue (suite)

Propriété	Description
Total d'échecs de l'authentification avant le verrouillage du compte utilisateur (*glide.zta.high_assurance.session.max.login.failed_attempts*)	Définissez le nombre maximal d'échecs de tentatives d'authentification avant que les utilisateurs ne soient déconnectés. **Remarque :** La valeur doit être comprise entre 3 et 10.
Propriétés d'audit	
Nombre total de jours pour conserver les enregistrements d'audit (*glide.zta.continuous_authentication.audit.lifespan*)	Spécifiez le nombre de jours pendant lesquels vous souhaitez enregistrer les enregistrements d'audit pour CA. **Remarque :** La valeur doit être comprise entre 1 et 180.
Nombre total de non. Nombre de jours après lesquels les politiques seront supprimées après leur désactivation (*glide.zta.continuous_authentication.policy.lifespan*)	Spécifiez le nombre de jours après lesquels les politiques CA sont supprimées.

Important :

- Par défaut, les sessions d'assurance élevée ne sont pas requises pour les sessions d'application mobile, même lorsqu'une politique d'authentification continue est active sur la source. Pour modifier ce comportement et bloquer l'accès à partir de sessions d'application mobile, mettez à jour la valeur de la propriété **glide.zta.high_assurance.mobile.session.allowed** sur `faux`.
- Les tables **sys_properties**, **sys_continuous_auth_policysys_user** sont exclues pour l'autorité de certification et ne peuvent pas être ajoutées à la configuration de la politique de l'autorité de certification.

Information associée

Explorer l'authentification continue

Politiques

Mesures

Travail préalable pour l'authentification continue

Travail préalable pour l'authentification continue

Assurez-vous d'effectuer le travail préalable suivant avant d'utiliser l'authentification continue (CA).

CA repose sur ServiceNow l'architecture de sécurité d'accès Zero Trust de qui vise à améliorer la sécurité en veillant à ce que l'utilisateur reste celui qu'il prétend être, même après le processus d'authentification initial.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.

La configuration CA peut être effectuée en fonction des éléments suivants :

- Connexion LDAP ou locale (nom d'utilisateur et mot de passe)
- Connexion SSO (SAML ou OIDC).

CA pour connexion locale

Lorsque les utilisateurs se connectent localement et pour vérifier leur identité, la MFA est utilisée comme mécanisme d'authentification. Si les utilisateurs n'ont pas configuré la MFA, il est obligatoire de terminer la configuration.

Remarque :

- Depuis Yokohama, la MFA est appliquée aux utilisateurs pour chaque connexion afin d'effectuer ServiceNow une connexion locale.
- Assurez-vous que les propriétés MFA sont actives et configurées en fonction de vos besoins. Pour en savoir plus sur les propriétés MFA, reportez-vous à la section Propriétés système de l'authentification multifacteur.

Pour en savoir plus, reportez-vous à la section Session d'assurance élevée pour une connexion non-SSO.

CA pour connexion SSO

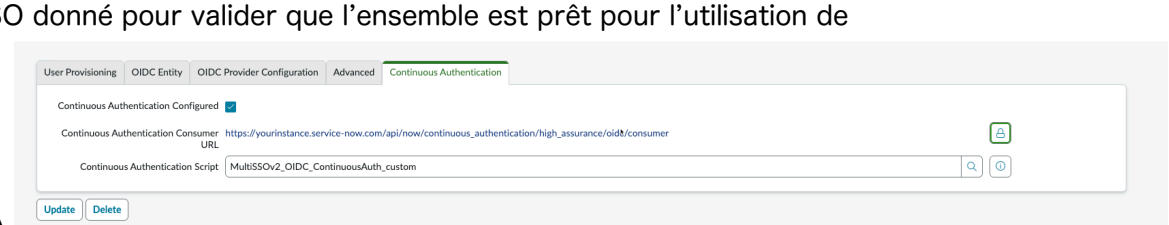
Lorsque les utilisateurs effectuent une connexion basée sur SSO (SAML ou OIDC). Pour vérifier l'identité des utilisateurs, la même SSO utilisée lors de la connexion initiale est affichée comme la revérification avec réauthentification ou MFA d'IdP.

Remarque :

- Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.
- Activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (*com.snc.integration.sso.multi.installer*).

Vous devez configurer l'IDP pour l'autorité de certification comme suit :

- Cochez la case qui doit être définie sur un enregistrement Multi SSO donné pour valider que l'ensemble est prêt pour l'utilisation de CA.



- Pour OIDC, l'autorité de certification repose sur une redirection vers le point de terminaison api/now/continuous_authentication/high_assurance/oidc/consumer , qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

doit être configuré sur l'IDP. Les options de réauthentification et de MFA d'IdP sont disponibles.

- Pour SAML, les enregistrements SSO utilisent le script de réagrégation par défaut pour tous les fournisseurs d'identité (IdP) afin de prendre en charge la nouvelle authentification.

Remarque :

- Pour configurer le step up pour **Okta** , vous pouvez utiliser le **ContinuousAuth_Okta_StepUp_Script** dans l'enregistrement IdP. Pour en savoir plus, consultez cette documentation .
- Pour configurer l'étape supérieure pour **Entra ID** ou **Azure** , vous pouvez utiliser le **ContinuousAuth_Azure_StepUp_Script** et ajouter la déclaration requise. Pour en savoir plus, consultez cette documentation .

Pour en savoir plus, reportez-vous à la section Niveau d'assurance élevé pour la connexion SSO.

Information associée

Explorer l'authentification continue

Activation de l'authentification continue

Configuration de l'authentification continue

Activation de l'authentification continue

Pour activer la fonctionnalité d'authentification continue sur votre instance, installez le module d'extension **Zero Trust - Continuous Authentication** (com.snc.zero_trust_continuous_authentication).

Avant de commencer

Rôle requis : admin

Ce module d'extension permet aux administrateurs de sécurité de définir des politiques de sécurité qui nécessitent une authentification renforcée (MFA) ou une nouvelle authentification (SSO) au sein d'une session connectée, en fonction des données auxquelles l'utilisateur accède et des activités qu'il effectue.

Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension **Authentification Zero Trust - continue** (com.snc.zero_trust_continuous_authentication) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Information associée

Travail préalable pour l'authentification continue

Configuration de l'authentification continue

Session d'assurance élevée avec authentification continue

Configuration de l'authentification continue

Configurez des politiques d'authentification continue (CA) pour authentifier à nouveau les utilisateurs en cas de tentative d'accès aux ressources que vous protégez.

Avant de commencer

- Rôle requis : admin (ca_admin)

Remarque :
Vous devez élever votre rôle à **ca_admin**.

- Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.
- Activez la propriété système Authentification continue (*glide.zta.continuous_authentication.enabled*). Pour plus d'informations, consultez Propriétés système.
- Activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (*com.snc.integration.sso.multi.installer*).
- Comprendre le travail préalable requis avant de configurer l'autorité de certification pour l'instance. Pour plus d'informations, consultez Travail préalable pour l'authentification continue.
- Les politiques CA peuvent être configurées pour une classe ou une table de données.

Procédure

1. Accédez à la **Tous** > **Authentification continue**.
2. Sélectionnez **l'onglet Politiques** .
3. Sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire :

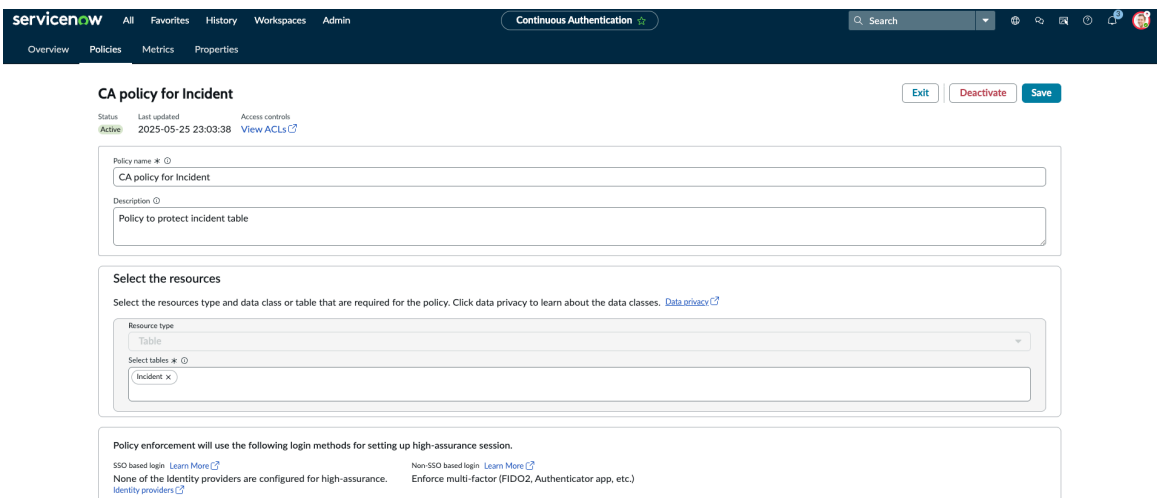
Authentification continue

Champ	Description
Nom de la politique	Nom de la politique
Description	Description générique de la politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner les ressources	Options : ○ **Classe de données**. Vous pouvez créer une classe de données et l'utiliser pour la configuration de la politique CA. **Remarque :** Pour en savoir plus sur la création d'une classe de données, reportez-vous à la section Classification des données. ○ **Table** **Remarque :** ○ La table sélectionnée avec des métadonnées affiche une erreur. ○ Vous devez vérifier si vous souhaitez réellement restreindre l'accès à la table de métadonnées, car cela peut avoir un impact sur l'accès de configuration de vos utilisateurs. ○ Les tables **sys_properties**, **sys_continuous_auth_policysys_user** sont exclues pour l'autorité de certification et ne peuvent pas être ajoutées à la configuration de la politique de l'autorité de certification.

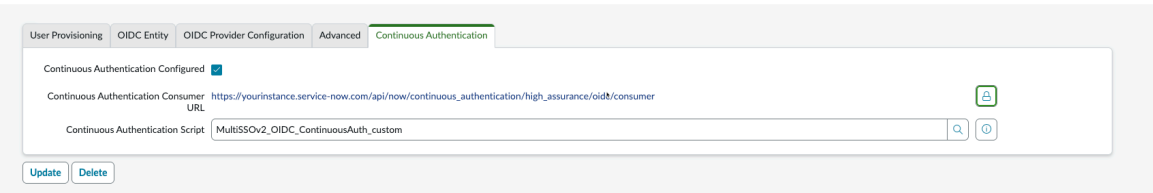


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez utiliser l'une des méthodes de connexion pour la politique CA :

- **Connexion basée sur SSO** : spécifiez les champs de l'onglet **Authentification continue** dans l'enregistrement du fournisseur d'identité et définissez l'enregistrement du fournisseur d'identité comme **actif**.



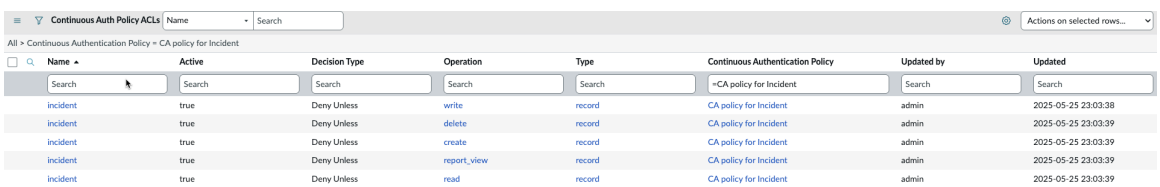
Pour en savoir plus sur la configuration des fournisseurs d'identité, consultez OIDC et SAML.

- **Connexion non basée sur SSO** : par défaut, s'il n'existe aucun fournisseur d'identité avec une configuration d'authentification continue, l'authentification multifacteur (MFA) est utilisée comme méthode de connexion. Assurez-vous que les propriétés MFA sont actives et configurées en fonction de vos besoins. Pour en savoir plus sur les propriétés MFA, reportez-vous à la section Propriétés système de l'authentification multifacteur.

5. Sélectionnez **Enregistrer et activer**.

Résultats

En fonction des détails fournis pour la configuration, la politique CA est créée avec une liste de contrôle d'accès (ACL) pour la table ou la classe de données sélectionnée. Vous pouvez afficher les détails des ACL créées en sélectionnant Afficher **les ACL** sur la page de politique.

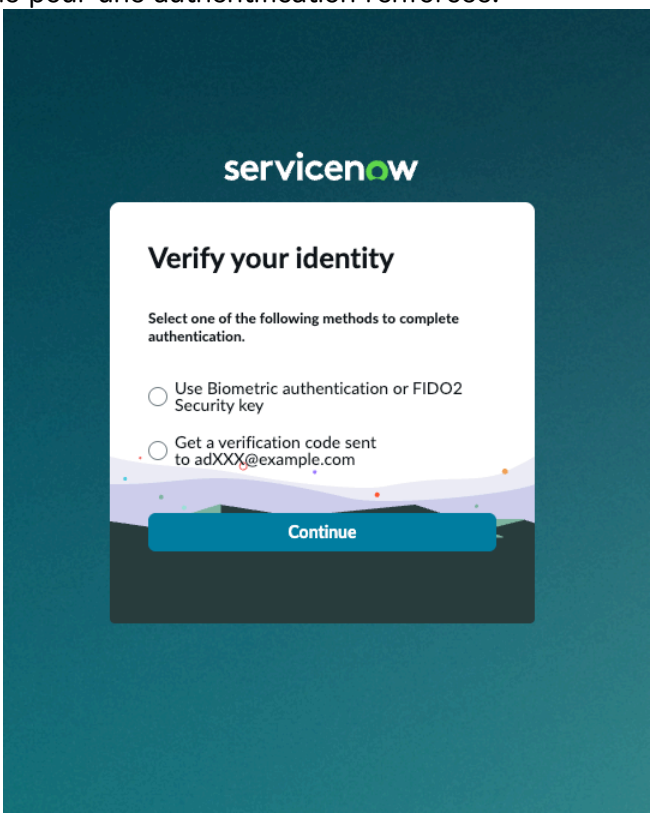


La politique CA créée invite l'utilisateur à s'authentifier pour accéder à la table ou à la classe de données que vous avez protégée à l'aide de la politique, en fonction des scénarios suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L’utilisateur qui s’est connecté en local pour se connecter à l’instance s’affiche avec la MFA de la plateforme pour une authentification renforcée.

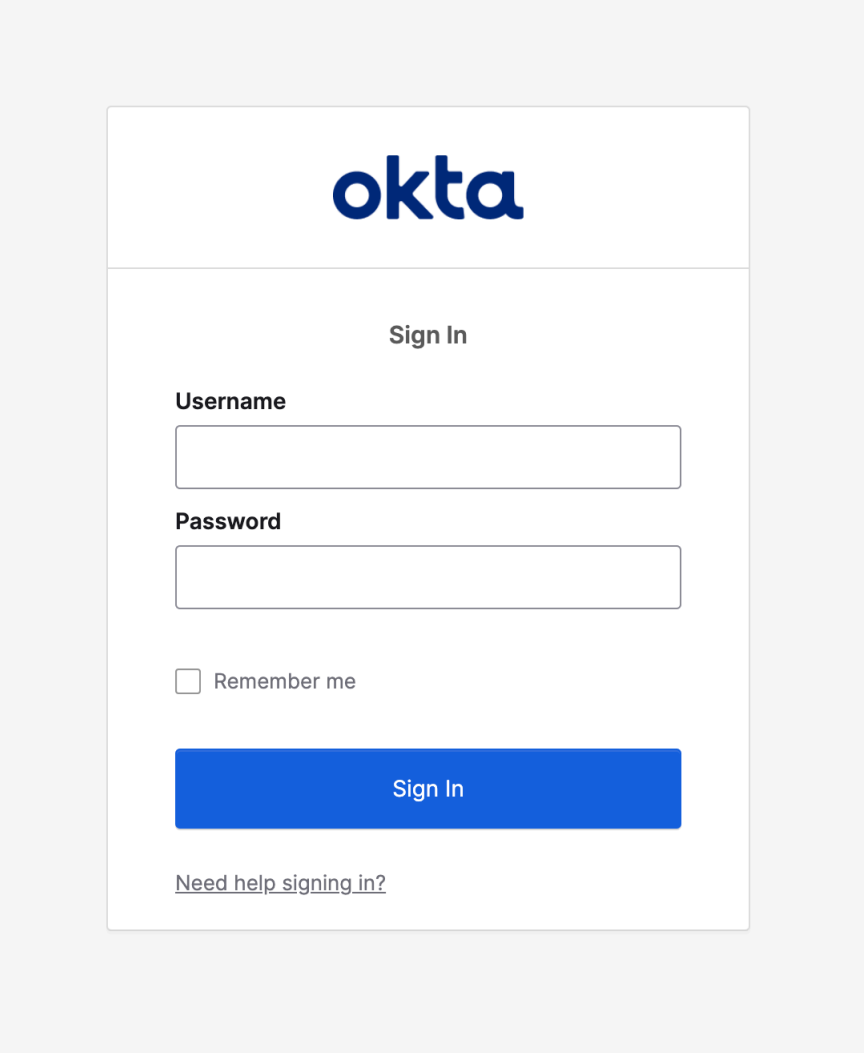


Remarque :
Le facteur MFA récemment utilisé par les utilisateurs s’affiche pour l’authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L’utilisateur qui a effectué une authentification unique (OIDC ou SAML) pour se connecter à l’instance s’affiche avec l’authentification unique pour une nouvelle authentification.



Une session d’assurance élevée est maintenant établie pour l’utilisateur. La session d’assurance élevée est limitée à la propriété système Durée de session d’assurance élevée (`glide.zta.high_assurance.session.timeout`). Si la durée de session d’assurance élevée dépasse la longueur de la propriété, l’utilisateur est invité à s’authentifier à nouveau ou à intensifier l’authentification.

Pour en savoir plus sur la configuration de bout en bout de l’authentification continue pour la table ou les données, consultez :

- Didacticiel : Configurer l’authentification continue pour une table.
- Didacticiel : Configurer l’authentification continue pour une classe de données.

Information associée

Explorer l’authentification continue

Travail préalable pour l’authentification continue

Activation de l’authentification continue

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Didacticiel : Configurer l'authentification continue pour une table

Procédure qui décrit la configuration de bout en bout de la politique d'authentification continue pour une table et les impacts sur les utilisateurs dus aux changements de configuration.

Avant de commencer

- Rôle requis : admin (ca_admin)

> **Remarque :**
> Vous devez élever votre rôle à **ca_admin**.

- Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.
- Activez la propriété système Authentification continue (*`glide.zta.continuous_authentication.enabled`*). Pour plus d'informations, consultez Propriétés système.
- Activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (*`com.snc.integration.sso.multi.installer`*).
- Comprendre le travail préalable requis avant de configurer l'autorité de certification pour l'instance. Pour plus d'informations, consultez Travail préalable pour l'authentification continue.

Procédure

1. Accédez à la **Tous** > **Authentification continue**.
2. Sélectionnez **l'onglet Politiques** .
3. Sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire :

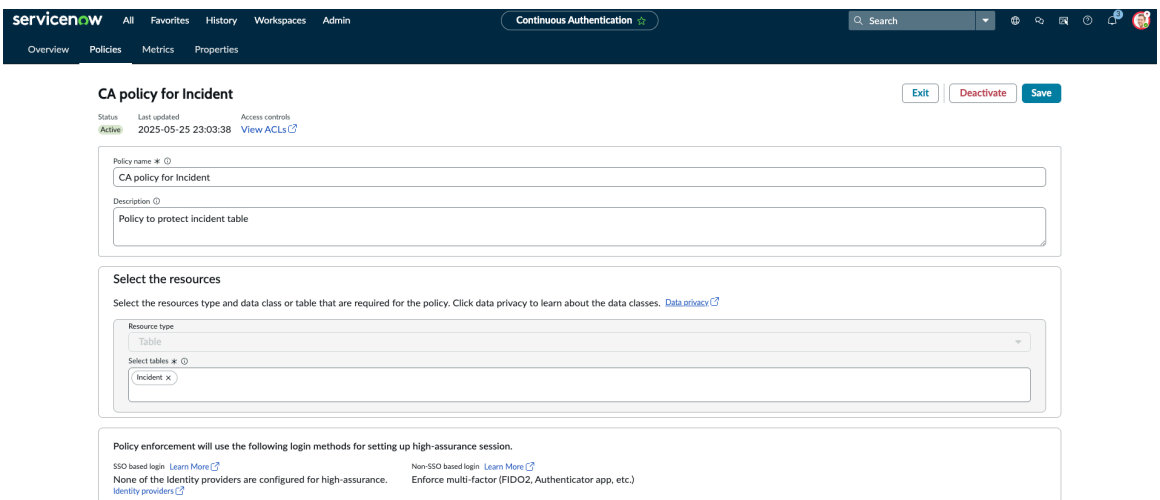
Authentification continue

Champ	Description
Nom de la politique	Nom de la politique
Description	Description générique de la politique
Sélectionner les ressources	Sélectionnez la **table**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ○ Dans cet exemple, la table **Incident** est sélectionnée. Vous pouvez sélectionner autant de tables que possible en fonction de vos besoins. ○ La table sélectionnée avec des métadonnées affiche une erreur. Vous devez vérifier si vous souhaitez réellement restreindre l'accès à la table de métadonnées, car cela peut avoir un impact sur l'accès de configuration de vos utilisateurs. ○ Les tables **sys_properties**, **sys_continuous_auth_policysys_user** sont exclues pour l'autorité de certification et ne peuvent pas être ajoutées à la configuration de la politique de l'autorité de certification.

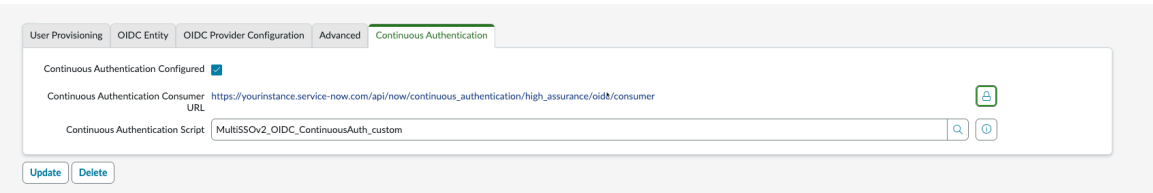


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez utiliser l'une des méthodes de connexion pour la politique CA :

- **Connexion basée sur SSO** : spécifiez les champs de l'onglet **Authentification continue** dans l'enregistrement du fournisseur d'identité et définissez l'enregistrement du fournisseur d'identité comme **actif**.



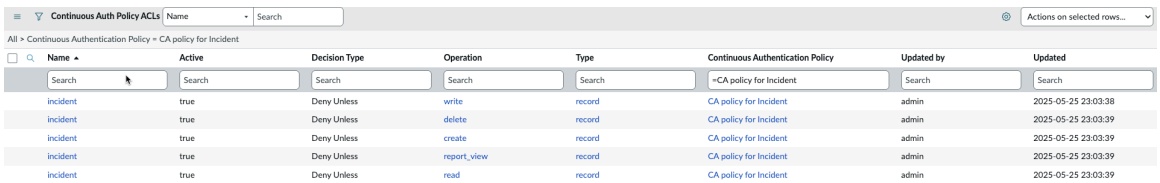
Pour en savoir plus sur la configuration des fournisseurs d'identité, consultez OIDC et SAML.

- **Connexion non basée sur SSO** : par défaut, s'il n'existe aucun fournisseur d'identité avec une configuration d'authentification continue, l'authentification multifacteur (MFA) est utilisée comme méthode de connexion. Assurez-vous que les propriétés MFA sont actives et configurées en fonction de vos besoins. Pour en savoir plus sur les propriétés MFA, reportez-vous à la section Propriétés système de l'authentification multifacteur.

5. Sélectionnez **Enregistrer et activer**.

Résultats

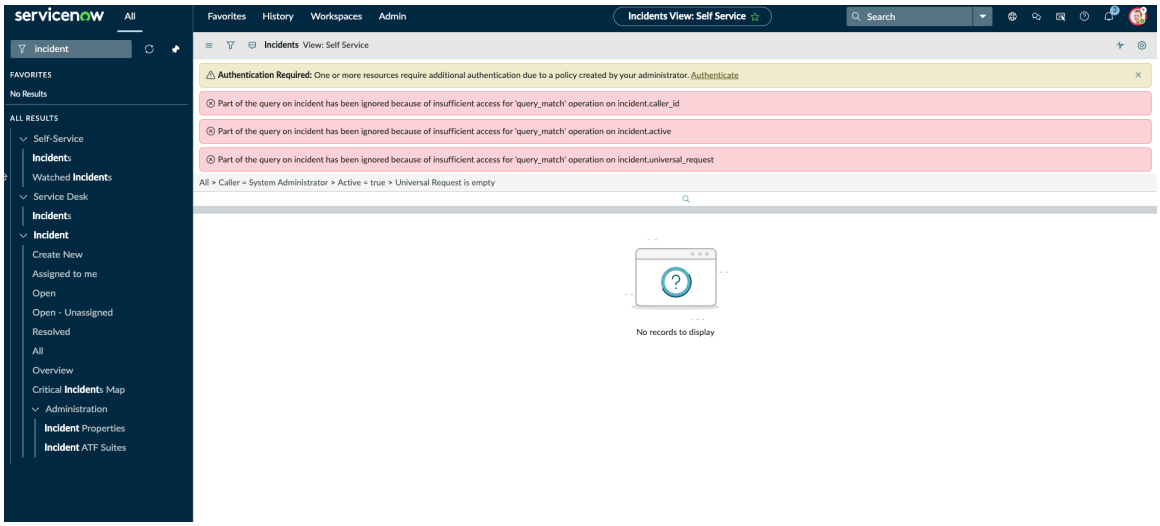
En fonction des détails fournis pour la configuration, la politique CA est créée avec une liste de contrôle d'accès (ACL) pour la table ou la classe de données sélectionnée. Vous pouvez afficher les détails des ACL créées en sélectionnant Afficher **les ACL** sur la page de politique.



La politique CA créée invite l'utilisateur à s'authentifier pour accéder à la table (dans ce cas, la table **Incident**) que vous avez protégée à l'aide de la politique. Les utilisateurs peuvent sélectionner **l'option Authentifier** .

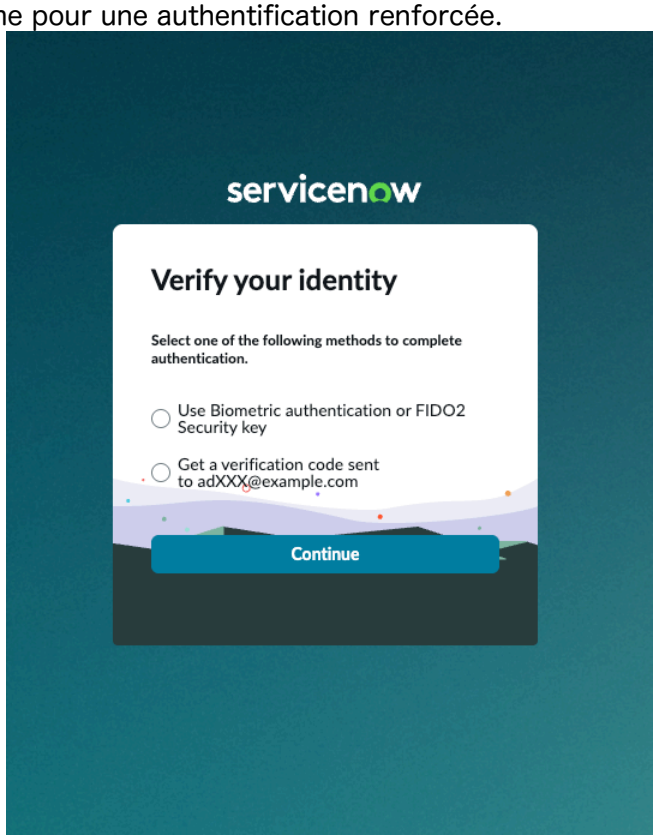
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Effectuez l'authentification basée sur les éléments suivants :

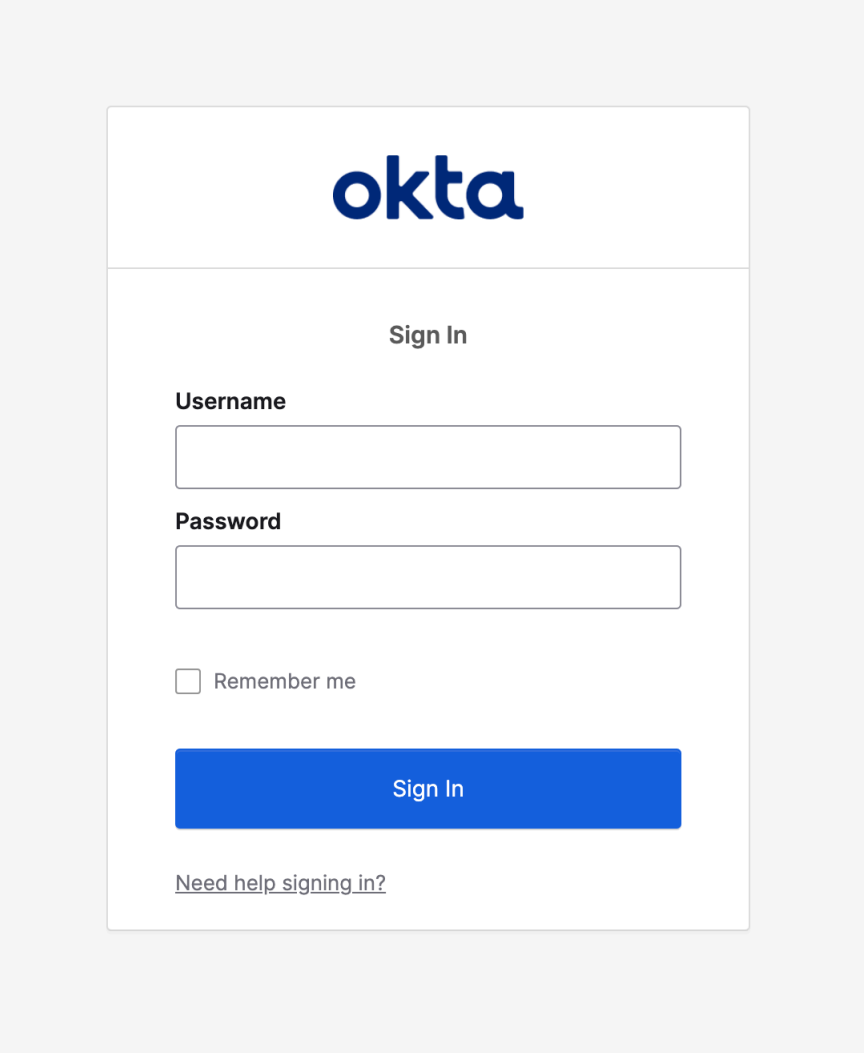
- L'utilisateur qui s'est connecté en local pour se connecter à l'instance s'affiche avec la MFA de la plateforme pour une authentification renforcée.



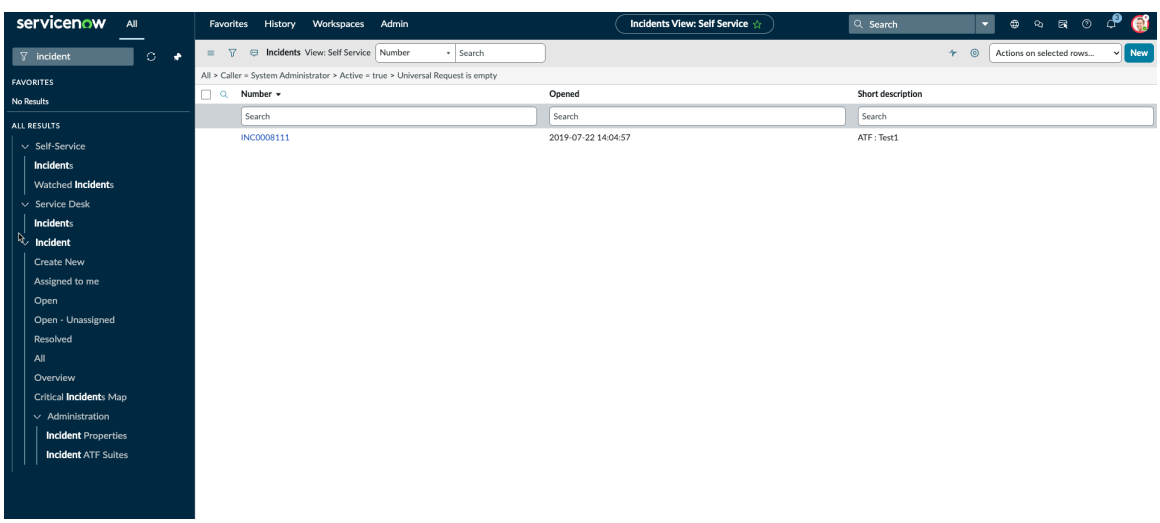
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L’utilisateur qui a effectué une authentification unique (OIDC ou SAML) pour se connecter à l’instance s’affiche avec l’authentification unique pour une nouvelle authentification.



Une fois l’authentification réussie, la table s’affiche.



Une session d’assurance élevée est maintenant établie pour l’utilisateur. La session d’assurance élevée est limitée à la propriété système Durée de session d’assurance élevée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(*glide.zta.high_assurance.session.timeout*). Si la durée de session d'assurance élevée dépasse la longueur de la propriété, l'utilisateur est invité à s'authentifier à nouveau ou à intensifier l'authentification.

Information associée

Configuration de l'authentification continue

Session d'assurance élevée avec authentification continue

Explorer l'authentification continue

Didacticiel : Configurer l'authentification continue pour une classe de données

Procédure qui décrit la configuration de bout en bout de la politique d'authentification continue pour une classe de données et les impacts sur les utilisateurs dus aux changements de configuration.

Avant de commencer

- Rôle requis : admin (ca_admin)

> **Remarque :**
> Vous devez élever votre rôle à **ca_admin**.

- Vous devez installer **l'authentification continue Zero Trust** (com.snc.zero_trust_continuous_authentication) pour choisir l'autorité de certification qui nécessite une licence.
- Activez la propriété système Authentification continue (*glide.zta.continuous_authentication.enabled*). Pour plus d'informations, consultez Propriétés système.
- Activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (*com.snc.integration.sso.multi.installer*).
- Comprendre le travail préalable requis avant de configurer l'autorité de certification pour l'instance. Pour plus d'informations, consultez Travail préalable pour l'authentification continue.

Procédure

1. Accédez à la **Tous** > **Authentification continue**.
2. Sélectionnez **l'onglet Politiques** .
3. Sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire :

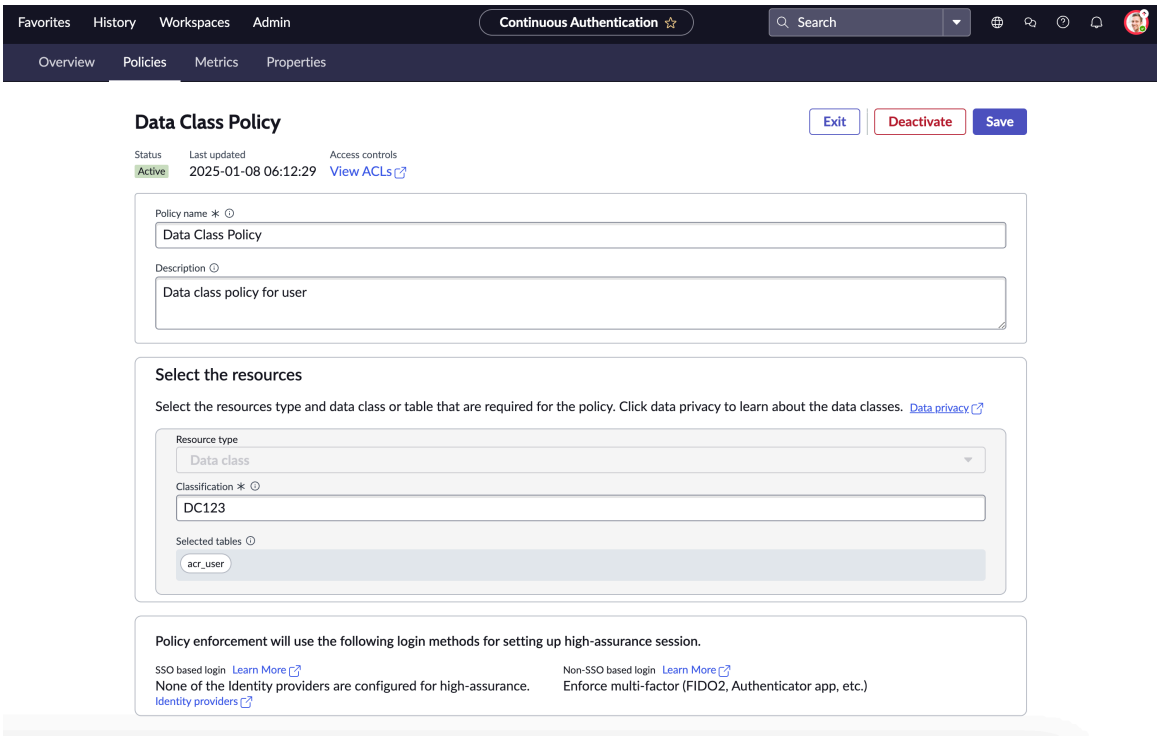
Authentification continue

Champ	Description
Nom de la politique	Nom de la politique
Description	Description générique de la politique
Sélectionner les ressources	Sélectionnez la **classe de données**. Vous pouvez créer une classe de données et l'utiliser pour la configuration de la politique CA.

Traduction automatique

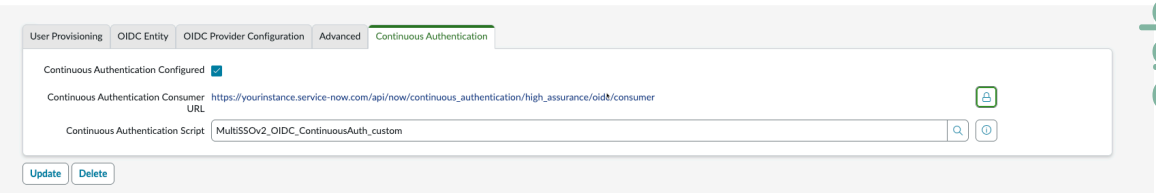
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Pour en savoir plus sur la création d'une classe de données, reportez-vous à la section Classification des données.



Remarque :
Vous pouvez utiliser l'une des méthodes de connexion pour la politique CA :

- **Connexion basée sur SSO** : spécifiez les champs de l'onglet **Authentification continue** dans l'enregistrement du fournisseur d'identité et définissez l'enregistrement du fournisseur d'identité comme **actif**.



  Pour en savoir plus sur la configuration des fournisseurs d'identité, consultez OIDC et SAML.

- **Connexion non basée sur SSO** : par défaut, s'il n'existe aucun fournisseur d'identité avec une configuration d'authentification continue, l'authentification multifacteur (MFA) est utilisée comme méthode de connexion. Assurez-vous que les propriétés MFA sont actives et configurées en fonction de vos besoins. Pour en savoir plus sur les propriétés MFA, reportez-vous à la section Propriétés système de l'authentification multifacteur.

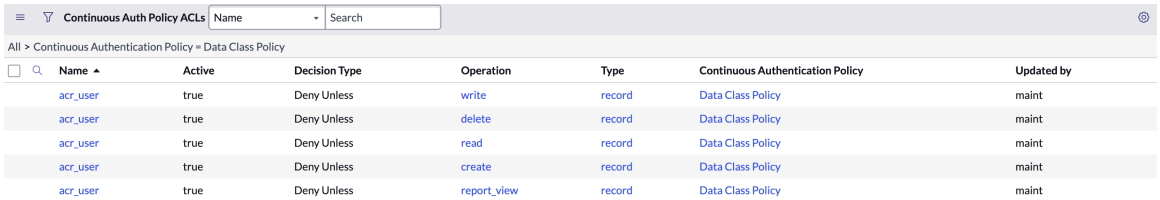
5. Sélectionnez **Enregistrer et activer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

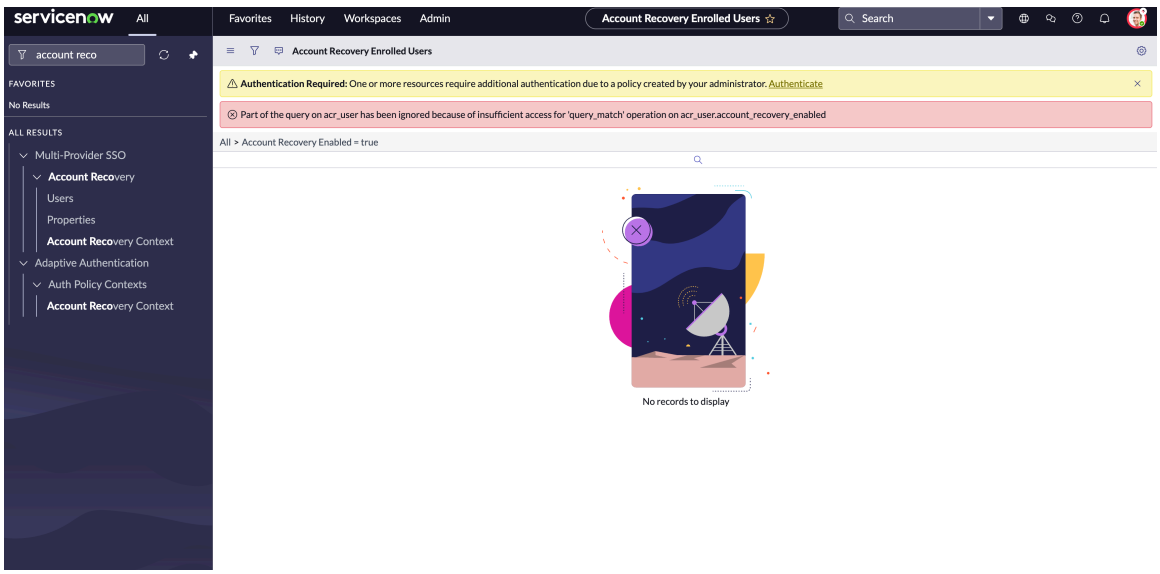
Résultats

En fonction des détails fournis pour la configuration, la politique CA est créée avec une liste de contrôle d'accès (ACL) pour la table ou la classe de données sélectionnée. Vous pouvez afficher les détails des ACL créées en sélectionnant Afficher **les ACL** sur la page de politique.



Name	Active	Decision Type	Operation	Type	Continuous Authentication Policy	Updated by
acr_user	true	Deny Unless	write	record	Data Class Policy	maint
acr_user	true	Deny Unless	delete	record	Data Class Policy	maint
acr_user	true	Deny Unless	read	record	Data Class Policy	maint
acr_user	true	Deny Unless	create	record	Data Class Policy	maint
acr_user	true	Deny Unless	report_view	record	Data Class Policy	maint

La politique CA créée invite l'utilisateur à s'authentifier auprès de la classe de données (dans ce cas, la classe de données définie pour la table **Récupération de compte**) que vous avez protégée à l'aide de la politique. Les utilisateurs peuvent sélectionner **l'option Authentifier** .

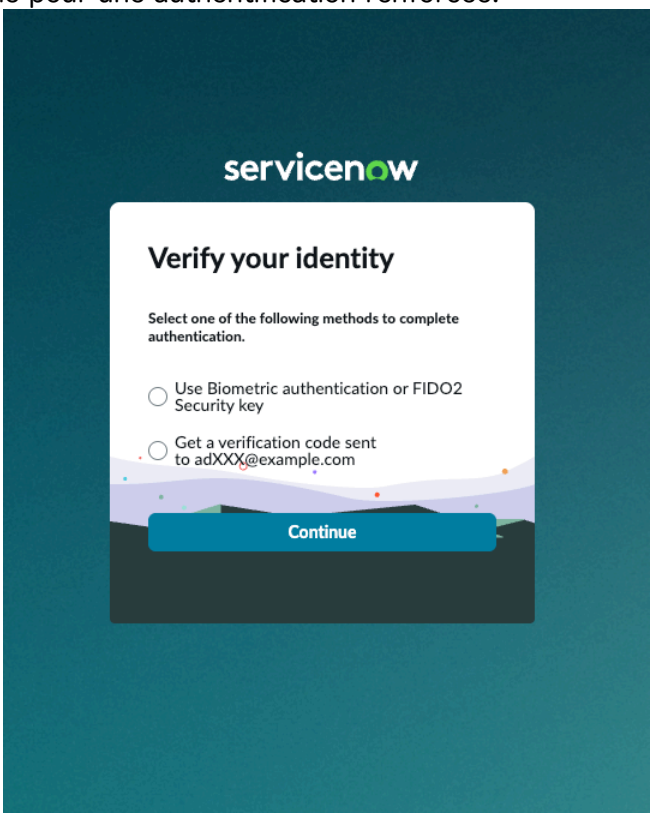


Effectuez l'authentification basée sur les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

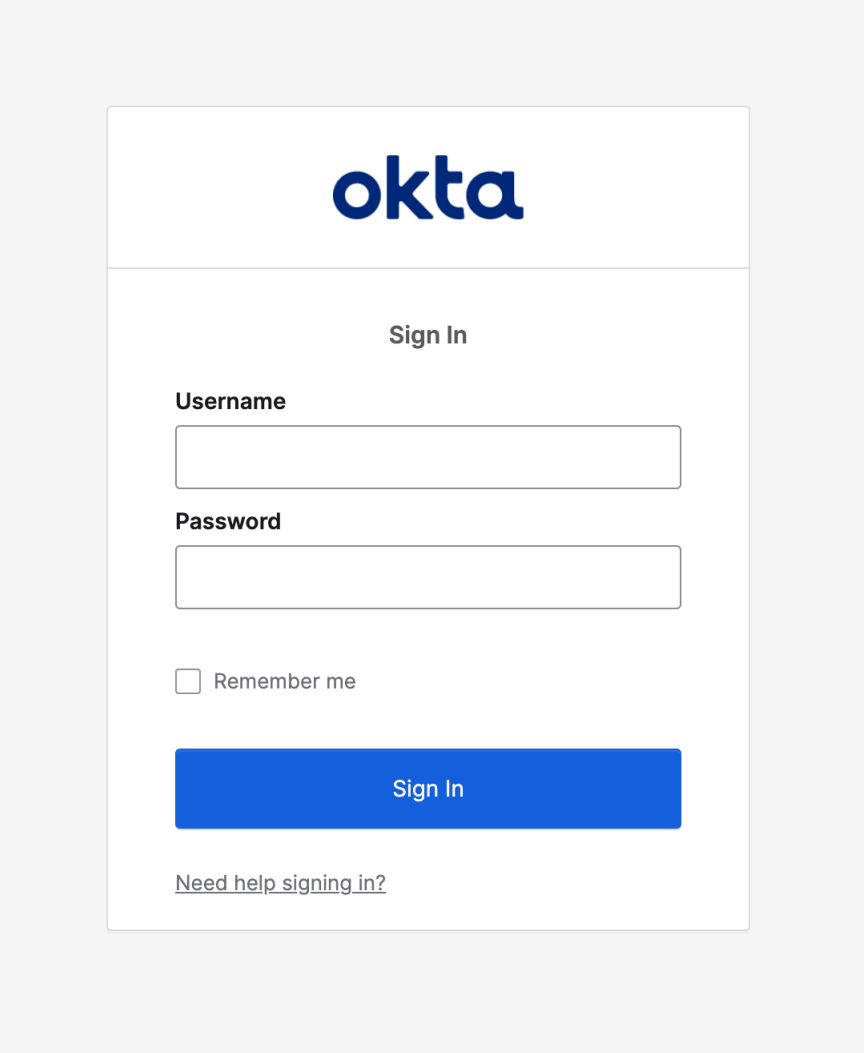
- L’utilisateur qui s’est connecté en local pour se connecter à l’instance s’affiche avec la MFA de la plateforme pour une authentification renforcée.



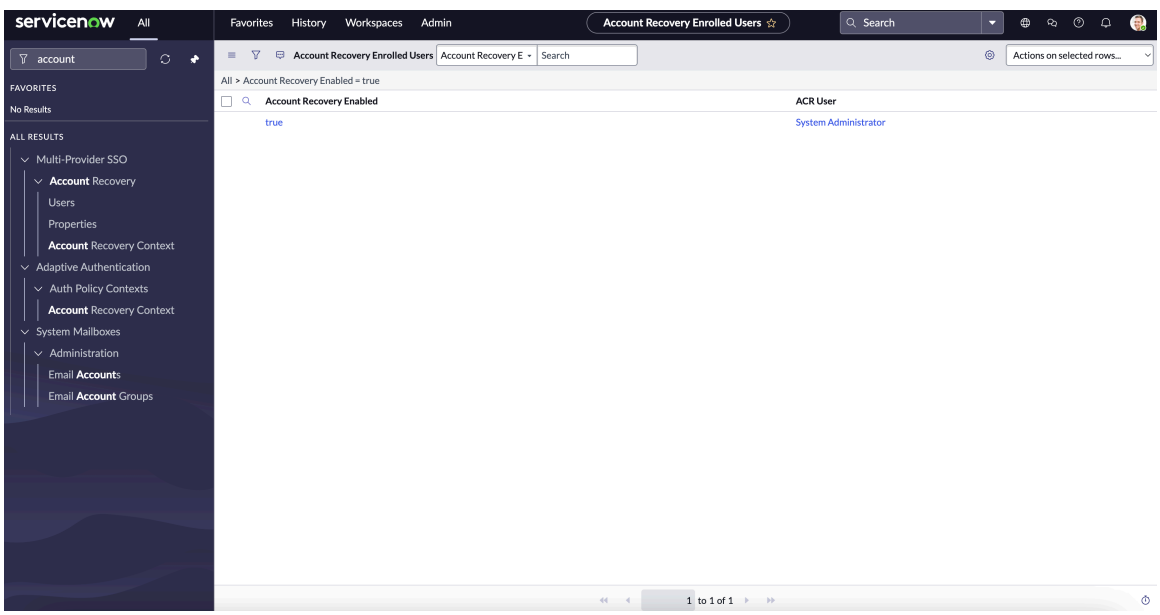
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L’utilisateur qui a effectué une authentification unique (OIDC ou SAML) pour se connecter à l’instance s’affiche avec l’authentification unique pour une nouvelle authentification.



Une fois l’authentification réussie, la table avec la classe de données s’affiche.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une session d'assurance élevée est maintenant établie pour l'utilisateur. La session d'assurance élevée est limitée à la propriété système Durée de session d'assurance élevée (`glide.zta.high_assurance.session.timeout`). Si la durée de session d'assurance élevée dépasse la longueur de la propriété, l'utilisateur est invité à s'authentifier à nouveau ou à intensifier l'authentification.

Information associée

Configuration de l'authentification continue

Session d'assurance élevée avec authentification continue

Explorer l'authentification continue

Session d'assurance élevée avec authentification continue

Établir une session d'assurance élevée pour avec ServiceNow authentification continue de .

Une session d'assurance élevée est une mesure de sécurité visant à établir une connexion sécurisée et de confiance avec les identités (utilisateurs) qui accèdent aux données et qui sont vérifiées avec un haut degré de confiance.

ServiceNow L'assurance élevée de est obtenue grâce à des méthodes d'authentification robustes qui appliquent une nouvelle authentification à l'aide de méthodes telles que l'authentification multifacteur (MFA) et l'authentification unique (SSO) pendant que les utilisateurs tentent d'accéder à des données sensibles.

Lorsque l'utilisateur s'authentifie à nouveau ou effectue une authentification renforcée (MFA), une session d'assurance élevée est établie, qui permet aux utilisateurs d'accéder aux données protégées par l'administrateur de l'autorité de certification en fonction de la configuration de la politique de l'autorité de certification.

Voici les méthodes de réauthentification utilisées pour établir un niveau d'assurance élevé en fonction du type de connexion :

- Niveau d'assurance élevé pour la connexion SSO
- Niveau d'assurance élevé pour une connexion sans SSO

La durée de validité de la session d'assurance élevée créée par l'utilisateur est basée sur la durée de session d'assurance élevée (`glide.zta.high_assurance.session.timeout`) déterminée par l'administrateur de l'autorité de certification.

La session d'assurance élevée peut être personnalisée en fonction de vos besoins en définissant les propriétés système **d'assurance élevée** :

Propriétés système à assurance élevée

Champ	Description
Durée de la session d'assurance élevée (`glide.zta.high_assurance.session.timeout`)	Spécifiez la durée de la session d'assurance élevée, après laquelle les utilisateurs finaux doivent s'authentifier à nouveau. Par défaut : 30 minutes. **Remarque :** La valeur doit être comprise entre 1 et 480.
Durée de session d'assurance élevée par défaut lors de la connexion	Spécifiez la durée en minutes de la durée de session à assurance élevée par défaut à compter de la connexion de l'utilisateur. Valeur par défaut : **5** minutes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

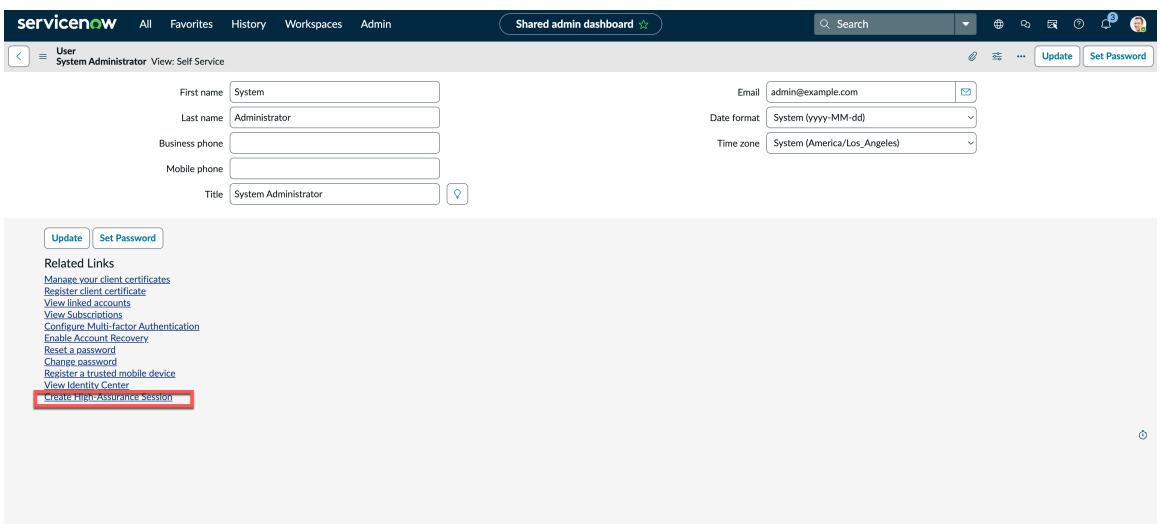
Propriétés système à assurance élevée (suite)

Champ	Description
	Remarque : Cette propriété ne s'applique qu'aux connexions non SSO.
Configurer le message d'affichage de l'utilisateur final (*glide.zta.high_assurance.session.message*)	Spécifiez le message qui s'affiche à l'utilisateur final pour une nouvelle authentification. Message par défaut : une ou plusieurs ressources nécessitent une authentification supplémentaire en raison d'une politique créée par votre administrateur.
Total d'échecs de l'authentification avant le verrouillage du compte utilisateur (*glide.zta.high_assurance.session.max.login.failed_attempts*)	Définissez le nombre maximal d'échecs de tentatives d'authentification avant que les utilisateurs ne soient déconnectés. **Remarque :** La valeur doit être comprise entre 3 et 10.

Session d'assurance élevée comme mesure préventive

Les utilisateurs qui travaillent avec des données à privilèges élevés telles que les transactions financières, les informations gouvernementales, les informations personnelles, peuvent établir une session d'assurance élevée comme mesure préventive pour éviter des notifications d'authentification fréquentes pendant leur session connectée.

Une session d'assurance élevée peut être créée par eux-mêmes. Pour créer une session d'assurance élevée, sélectionnez **Profil d'utilisateur** > **Profil**. Dans la section **Liens connexes** , sélectionnez **Créer une session d'assurance élevée**. Vérifiez votre identité pour créer une session d'assurance élevée.



Information associée

- Explorer l'authentification continue
- Travail préalable pour l'authentification continue
- Configuration de l'authentification continue

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau d’assurance élevé pour la connexion SSO

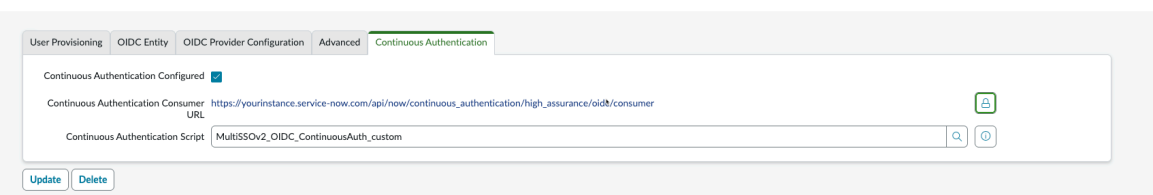
Établissez une session d’assurance élevée pour la connexion SSO à l’aide de l’authentification ServiceNow continue de .

Une session d’assurance élevée est une session qui exige qu’un utilisateur vérifie son identité et s’authentifie auprès d’une identité ou de fournisseurs d’identité spécifiques pendant une période spécifique.

ServiceNow La fonctionnalité d’authentification continue (CA) de vous permet de créer des politiques qui créent une session d’assurance élevée pour les utilisateurs qui accèdent aux informations personnelles identifiables (PII) et aux données sensibles, ou qui limitent l’accès aux données explicites que vous souhaitez protéger.

Lorsque l’utilisateur s’authentifie à nouveau, une session de haute assurance est établie, qui permet aux utilisateurs d’accéder aux données protégées par l’administrateur de l’autorité de certification en fonction de la configuration de la politique de l’autorité de certification.

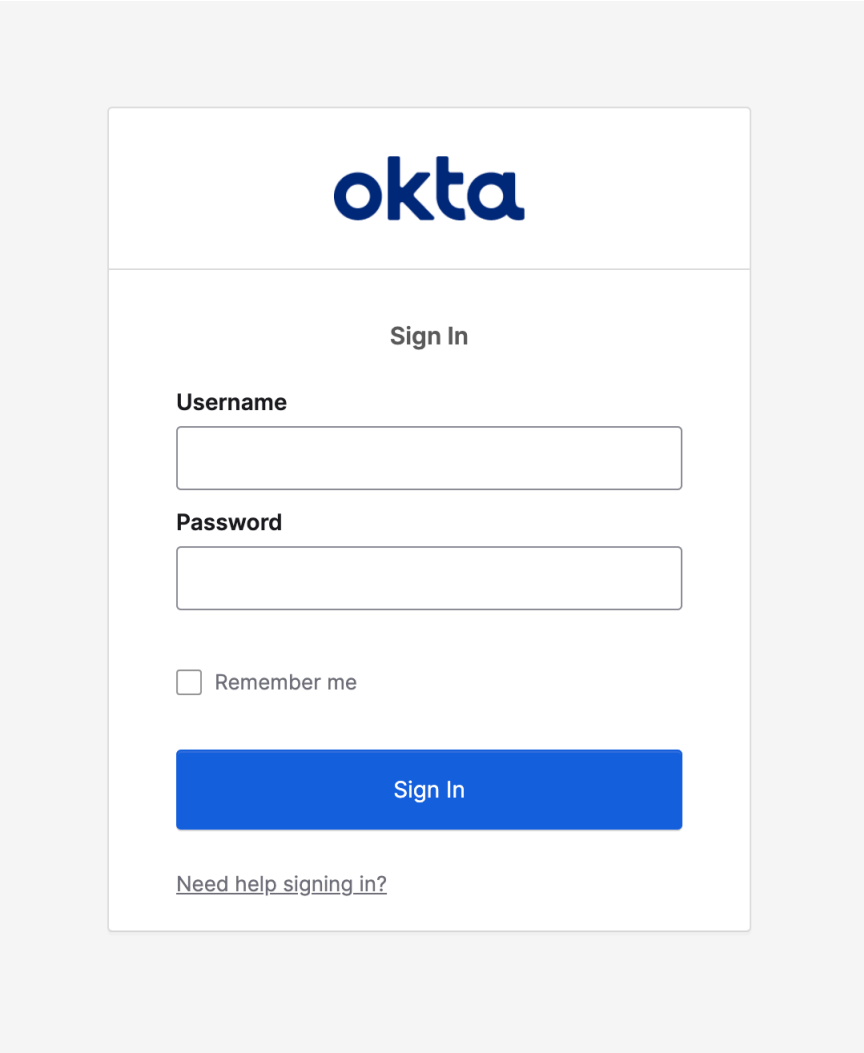
Vous pouvez créer des politiques CA pour vérifier l’identité des utilisateurs et autoriser les utilisateurs à accéder aux données que vous avez protégées. Vous pouvez configurer la politique de l’autorité de certification et fournir les détails des fournisseurs d’identité dans l’enregistrement des fournisseurs d’identité pour établir une session d’assurance élevée.



Les utilisateurs qui effectuent une connexion basée sur SSO (SAML ou OIDC) et chaque fois qu’il y a une tentative d’accès aux données protégées, l’écran de nouvelle authentification est demandé avec le même SSO que celui utilisé par l’utilisateur lors de la connexion initiale.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois l'authentification SSO réussie, les données protégées sont affichées aux utilisateurs pendant un certain laps de temps. Vous pouvez configurer les propriétés pour modifier la limite de temps en fonction de vos besoins. Pour en savoir plus, reportez-vous à la section Session d'assurance élevée avec authentification continue.

La réauthentification avec une connexion SSO (SAML ou OIDC) crée une session d'assurance élevée établissant une connexion sécurisée et de confiance avec les identités (utilisateurs) qui accèdent aux données protégées.

Une session d'assurance élevée établie pour l'utilisateur est limitée à la propriété système Durée de session d'assurance élevée (`glide.zta.high_assurance.session.timeout`). Si la durée de session d'assurance élevée dépasse la longueur de la propriété, l'utilisateur est invité à s'authentifier à nouveau ou à intensifier l'authentification.

Information associée

- Session d'assurance élevée avec authentification continue
- Travail préalable pour l'authentification continue
- Configuration de l'authentification continue

Session d'assurance élevée pour une connexion non-SSO

Établissez une session d'assurance élevée pour les connexions non-SSO (locales ou LDAP) à l'aide de l'authentification ServiceNow continue de .

Traduction automatique

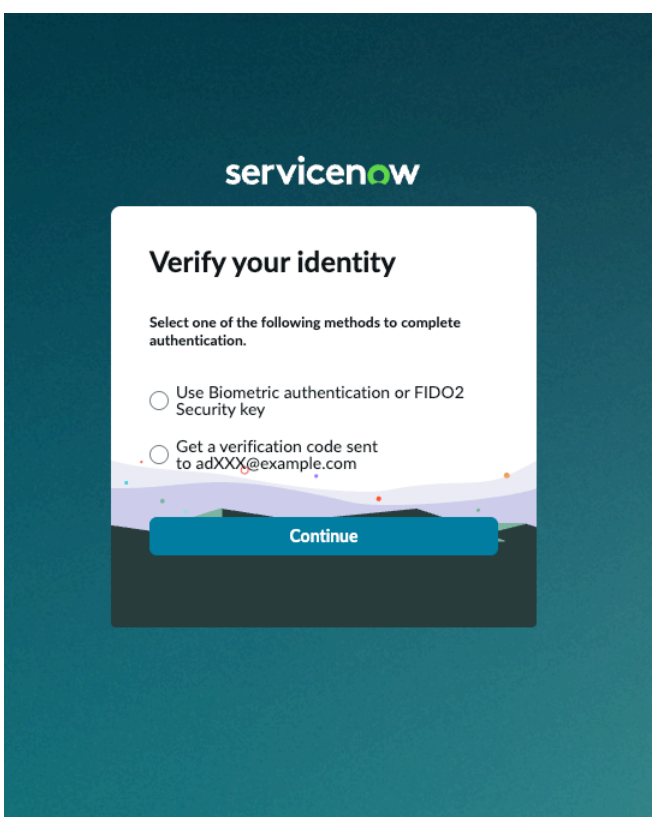
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une session d'assurance élevée est une session qui exige qu'un utilisateur vérifie son identité et s'authentifie auprès d'une identité ou de fournisseurs d'identité spécifiques pendant une période spécifique.

ServiceNow La fonctionnalité d'authentification continue (CA) de vous permet de créer des politiques qui créent une session d'assurance élevée pour les utilisateurs qui accèdent aux informations personnelles identifiables (PII) et aux données sensibles, ou qui limitent l'accès aux données explicites que vous souhaitez protéger.

Lorsque l'utilisateur effectue une authentification renforcée (MFA), une session d'assurance élevée est établie, qui permet aux utilisateurs d'accéder aux données protégées par l'administrateur de l'autorité de certification en fonction de la configuration de la politique de l'autorité de certification.

Vous pouvez créer des politiques CA pour vérifier l'identité des utilisateurs et autoriser les utilisateurs à accéder aux données que vous avez protégées. Les utilisateurs qui effectuent une connexion non basée sur SSO (local ou LDAP) et chaque tentative d'accès aux données protégées, un écran d'authentification renforcée (MFA) s'affiche pour les utilisateurs.



Une fois l'authentification réussie, les données protégées sont affichées aux utilisateurs pendant un certain laps de temps. Vous pouvez configurer les propriétés pour modifier la limite de temps en fonction de vos besoins. Pour en savoir plus, reportez-vous à la section Session d'assurance élevée avec authentification continue.

Remarque :
Si les utilisateurs n'ont pas configuré la MFA, il est obligatoire de terminer la configuration.

L'authentification renforcée (MFA) crée une session d'assurance élevée qui établit une connexion sécurisée et de confiance avec les identités (utilisateurs) qui accèdent aux données protégées.

Une session d'assurance élevée établie pour l'utilisateur est limitée à la propriété système Durée de session d'assurance élevée (`glide.zta.high_assurance.session.timeout`). Si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la durée de session d’assurance élevée dépasse la longueur de la propriété, l’utilisateur est invité à s’authentifier à nouveau ou à intensifier l’authentification.

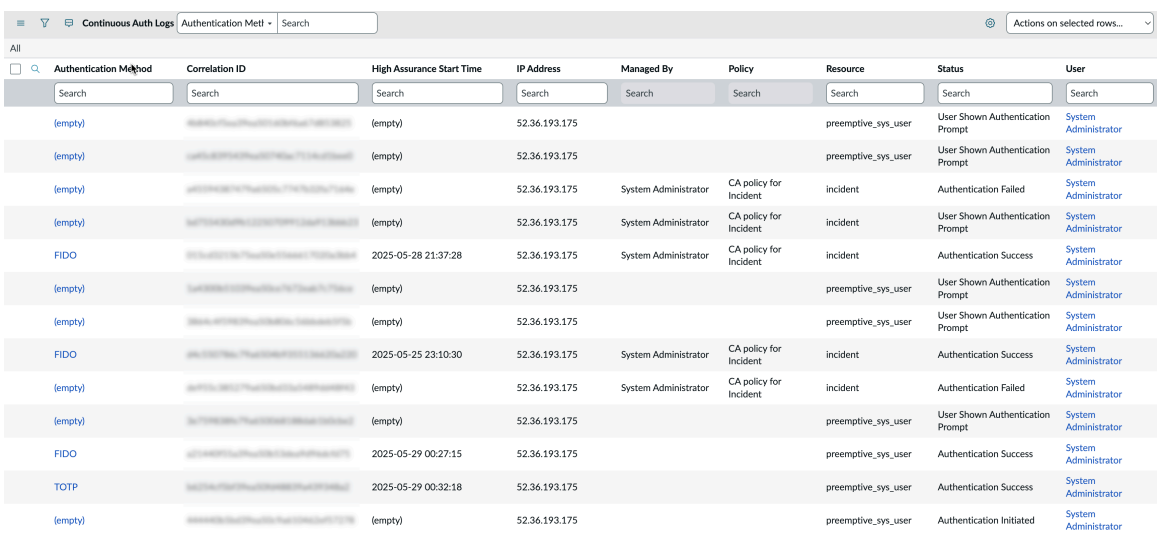
Information associée

- Session d’assurance élevée avec authentification continue
- Travail préalable pour l’authentification continue
- Configuration de l’authentification continue

Journaux d’audit de l’authentification continue

Décrit en détail les journaux d’authentification continue (CA). Les journaux CA affichent toutes les tentatives d’authentification effectuées par les utilisateurs.

Les informations d’audit du journal connexe de l’autorité de certification sont disponibles dans le **continuous_auth_log. LIST** . Vous pouvez taper **continuous_auth_log. LIST** dans la navigation pour afficher les journaux de l’autorité de certification.



La page de journal affiche des informations sur la méthode d’authentification, l’ID de corrélation, ainsi que d’autres détails relatifs à la session de l’utilisateur.

Domain Separation pour les fournisseurs de services

Grâce à la plateforme ServiceNow, les fournisseurs de services peuvent offrir à leurs clients une intégration plus rapide, assurer le respect de la conformité et protéger leurs données à l'aide de Domain Separation. Vous pouvez séparer les données, les processus et les rapports clients en groupes logiques appelés domaines. Les fournisseurs de services déterminent qui peut afficher tel ou tel contenu et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



En savoir plus sur la séparation en domaines.

Configurer



Configurez Séparation en domaines.

Référence



Obtenez des détails sur la séparation en domaines.

Analyser



En savoir plus sur l’analyse
de la séparation en domaines

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer la séparation de domaine

Avec Séparation de domaine, vous pouvez séparer les données, les processus et les tâches administratives en domaines définis de manière logique.

Séparation de domaine est préférable pour les clients qui :

- Nécessité d'appliquer une ségrégation absolue des données entre les entités d'entreprise (séparation des données).
- personnalisent les définitions des processus business et les interfaces utilisateur pour chaque domaine (administration déléguée) ;
- conservent certains processus globaux et des générations de rapports globaux dans une seule instance.
- Séparez les données entre les fournisseurs de services, les clients, les partenaires ou les sous-organisations.
- Présenter des différences de processus mineures ou modérées entre les clients.

Séparation de domaine comparée à des instances distinctes

Bien que Domain Separation fournisse une prise en charge partagée, le partage est toujours contenu dans une seule instance. Certaines données, propriétés et processus globaux sont partagés dans tous les domaines. Par exemple, le fait d'avoir le système *Se souvenir de moi* sur la page de connexion du système est global et ne peut pas être spécifié par domaine.

Si vous avez besoin d'une séparation complète et totale de toutes les propriétés système et que vous n'avez pas besoin de rapports globaux ou de processus globaux, des instances distinctes sont la meilleure option.

Séparation des données

Les membres d'un domaine ne voient que les données contenues dans leur domaine ou les domaines enfants qui sont plus bas dans la hiérarchie des domaines. Par défaut, tous les utilisateurs et tous les enregistrements sont membres du domaine global, sauf si un administrateur les affecte à un domaine particulier. Une fois que vous avez affecté un utilisateur ou un enregistrement à un domaine, l'instance compare le domaine de l'utilisateur au domaine de l'enregistrement pour déterminer si l'utilisateur peut afficher l'enregistrement.

Les applications ServiceNow sont définies avec les niveaux de prise en charge incrémentielle suivants. Ces niveaux sont basés sur la perspective des cas d'utilisation et des profils réels.

Séparation des données : les locataires ne voient que les données qu'ils ont l'autorisation de voir. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données du locataire s'ils n'y ont pas accès.

Séparation de l'interface utilisateur : prend en charge une expérience spécifique au locataire pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.

Séparation de la logique métier : vous pouvez créer des politiques système spécifiques au locataire, telles que des notifications par e-mail, des règles métier, des scripts clients, une politique d'interface utilisateur et des actions d'interface utilisateur.

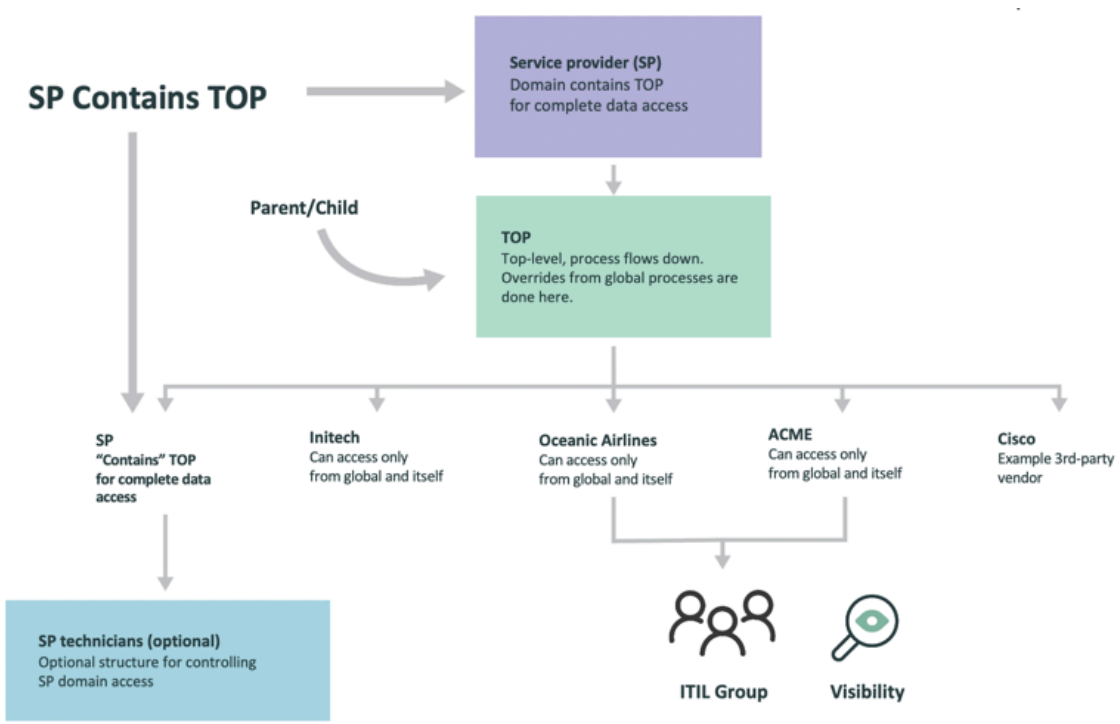
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modélisation hiérarchique : multi-location imbriquée afin que les locataires parents puissent accéder aux ressources des locataires enfants. La logique métier pour les locataires parents s'exécute automatiquement pour les locataires enfants et peut être remplacée à n'importe quel niveau.

Intelligence interlocataire (champ d'application de domaine) : gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires qui ont accès à des données de locataire supplémentaires.

En général, les données définies à un niveau supérieur dans la hiérarchie des domaines ne sont pas visibles aux niveaux inférieurs de la hiérarchie.



Migration du chemin de domaine

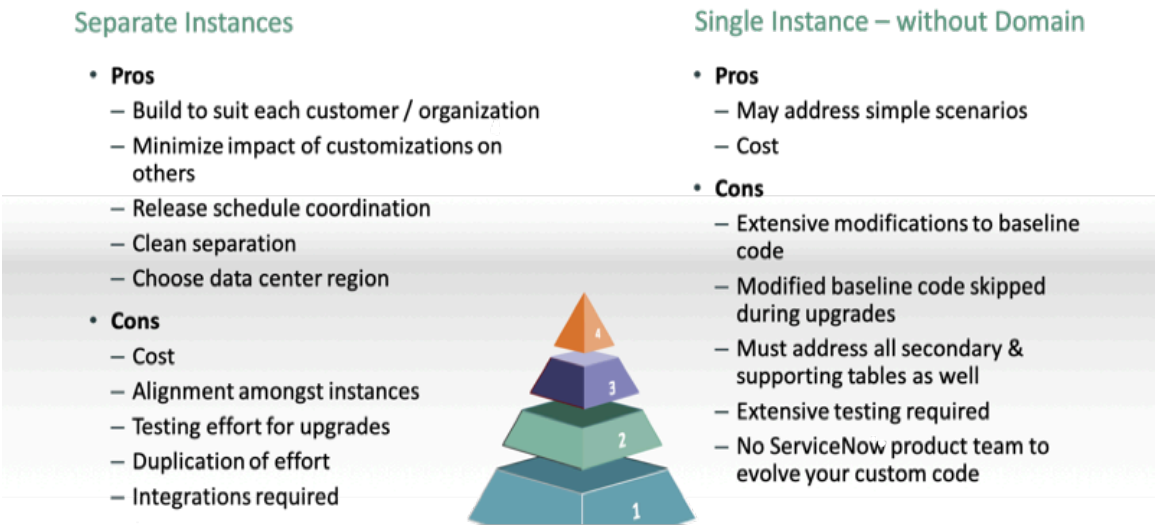
Les chemins de domaine sont utilisés pour tous les clients. La numérotation de domaine n'est pas utilisée. Service client et assistance peut aider à la mise à niveau.

Alternatives à la séparation en domaines

Des instances distinctes sont une alternative courante à la séparation de domaine. Cela offre un grand degré de flexibilité pour répondre aux exigences des clients et des parties prenantes, avec peu ou pas d'impact sur les autres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



⚠ Avertissement :
Avant d'activer la séparation par domaine, consultez votre représentant pour vérifier qu'elle est adaptée à votre environnement. Séparation de domaine ajoute un niveau de frais généraux d'administration. Bien qu'elle puisse être désactivée, elle ne peut pas être supprimée d'une instance.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Module d'extension Domain Separation

Configuration pouvant être déléguée à des clients internes ou externes

Séparation de domaine est conçue pour permettre ServiceNow® aux fournisseurs de services (SP) de configurer les services qu'ils offrent à leurs clients. Il n'est pas conçu pour permettre à leurs clients d'administrer eux-mêmes ces services, sauf dans quelques domaines que cette rubrique détaille.

Vue d'ensemble

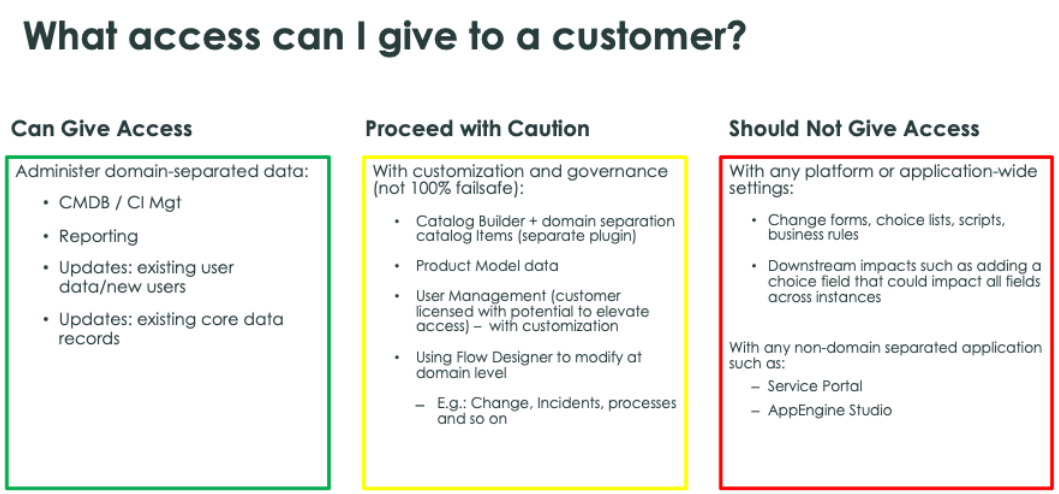
Il est sûr pour les clients SP, par eux-mêmes, de gérer les données contenues dans leur domaine qui n'affectent pas les licences ou les autres clients. Par exemple, un client peut créer de nouveaux rapports ou gérer des éléments de configuration en toute sécurité, mais il ne peut pas personnaliser des champs, des choix, des règles métier et d'autres processus dans lesquels ils peuvent avoir un impact sur d'autres clients sur la même instance.

Les ServiceNow rôles d'administration du système de base et leurs contrôles d'accès sur la ServiceNow plateforme sont conçus pour une seule équipe d'administrateurs par instance. Par exemple, le rôle domain_admin est accordé à l'une des ressources du SP pour gérer tous les paramètres de domaine de l'instance et pour créer de nouveaux domaines. Pour toutes les tâches d'administration spécifiques à un domaine, le SP doit créer de nouveaux rôles « administrateur client » et des contrôles d'accès selon les besoins pour accorder un accès spécifique à ses clients.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'image suivante est une vue d'ensemble des fonctions d'administration courantes dans différentes catégories de ce qui peut être fait en toute sécurité pour un client.



Peut donner accès

Exemples :

- Gestion des données CI dans la CMDB
- Création de rapport
- Mises à jour des données utilisateur existantes ou nouveaux utilisateurs sans rôles
- Mises à jour des enregistrements de données de base existants tels que département, groupe, emplacement, centre de coûts ou nouveaux groupes sans rôles, et nouveaux départements/centres de coûts/emplacement.

Procédez avec prudence

Exemples :

- Éléments de catalogue : pour créer des éléments de catalogue spécifiques au client qui peuvent être mis à jour par le client, deux options peuvent être utilisées ensemble : Séparation de domaine pour les éléments de catalogue (Séparation de domaine et Catalogue de services) permet au propriétaire de l'instance de créer des éléments dans le domaine du client. Le propriétaire de l'instance peut créer un rôle pour permettre aux clients de mettre à jour des champs sécurisés tels que le prix, la description et les images. Le générateur de catalogue (nouveau dans la version Quebec) donne à l'équipe d'administrateurs SP la possibilité de créer des modèles d'éléments qui peuvent être distribués en toute sécurité aux clients pour créer de nouveaux éléments dans leur domaine à partir d'une expérience d'interface utilisateur prescriptive.
- Gestion des utilisateurs/groupes : il est prudent de créer un rôle « administrateur client » qui peut créer et modifier des enregistrements d'utilisateurs, mais l'ajout et la suppression de rôles peuvent affecter la sécurité et la gestion des licences. Il n'y a aucun moyen dans le système de base de subdiviser les rôles qui sont sûrs pour qu'un client puisse les accorder. Il en va de même pour la création et la modification de groupes. Bien que le groupe lui-même puisse être modifié, l'ajout ou la soustraction de rôles doit être contrôlé.
- Flow Designer : ServiceNow Studio de workflow est l'outil de création utilisé pour créer un processus (workflow) pour les tables. Le rôle flow_designer donne aux clients un accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sans script aux flux de version. Ils peuvent lire et cloner tous les flux dans les domaines au-dessus d'eux dans la hiérarchie. Ils peuvent créer et modifier des flux dans leur domaine. Cela ne peut toutefois pas se faire en vase clos. Toute personne susceptible d'affecter le processus doit être ajoutée à l'équipe d'administration globale pour la gouvernance afin que les processus ne s'annulent pas ou ne provoquent pas d'autres conflits.

Ne pas donner accès

Comprendre le fonctionnement des champs de choix est utile pour comprendre pourquoi seule l'équipe d'administrateurs SP devrait les gérer.

- Structure d'un champ de choix : les valeurs de champ de choix sont stockées dans la table sys_choice et regroupées en fonction de : Table, Domaine et Langue.

  Par exemple, le champ **État** d'une tâche est disponible pour toutes les tables qui étendent une tâche. Cela signifie que chaque table peut avoir ses propres valeurs, ces valeurs peuvent être multipliées par domaine et les valeurs de domaine peuvent être multipliées par langue.

  Toutes les valeurs de **l'état** dans toutes les tables, domaines et langues sont considérées comme les valeurs du champ **État** .

- Fonctionnement des changements apportés aux champs de choix : lorsqu'un champ de choix est mis à jour, une charge utile est créée avec toutes les valeurs de ce champ (tables, domaines, langues). Lorsque vous installez cette charge utile sur une instance, toutes les valeurs existantes pour le champ sont supprimées et les nouvelles valeurs sont chargées. Cela garantit qu'il n'y a pas d'entrées en double ou de valeurs restantes qui ne sont plus valides.

  Pour cette raison, il est impossible de donner à un client dans une instance séparée par domaine la possibilité de mettre à jour directement les champs de choix, car cela affecterait l'ensemble de l'instance. En outre, vous ne pouvez pas mettre à jour les choix directement dans une instance de production, car les ensembles de mises à jour importés qui affectent ce champ remplaceraient les choix existants. Dans certains cas, les champs de choix peuvent piloter les processus eux-mêmes, qui s'interrompraient si un client devait modifier ces champs.

Pour en savoir plus, consultez :

- Exploring user administration
- Créer une règle ACL
- Parcours d'apprentissage du fournisseur de services sur ServiceNow University
- Domain Separation pour les fournisseurs de services
- Concepts des fournisseurs de services
- Assistance applicative pour Domain Separation
- Notes de publication de Domain Separation

Affectation de domaine

Par défaut, Séparation de domaine ajoute un champ de domaine aux tables et à leurs extensions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également étendre Séparation de domaine à toutes les nouvelles tables que vous créez en ajoutant un champ **sys_domain** à la définition de dictionnaire de la table. Par défaut, le domaine système uniquement sépare les tables de plateforme et d'application de base de référence, le cas échéant.

⚠ Avertissement :
ServiceNow ne recommande pas de séparer les tables de plateforme par domaine (toutes les tables portant le préfixe sys_, telles que les tables Entrée de dictionnaire [sys_dictionary] et Remplacement d'entrée de dictionnaire [sys_dictionary_override]), car cela peut produire des résultats inattendus.

Un seul domaine est affecté à chaque enregistrement.Ce domaine est stocké dans le champ **sys_domain**.Par défaut, plusieurs tables ont la colonne **sys_domain** et sont déjà séparées par domaine.

La valeur du champ **sys_domain** contient le domaine affecté à l'enregistrement par l'un des éléments suivants :

- Société à laquelle l'utilisateur appartient
- Règle métier lors de la création d'un enregistrement
- Module utilisé lors de la création de l'enregistrement
- Modèle de formulaire utilisé lors de la création d'un enregistrement
- Domaine de l'enregistrement parent
- Domaine affecté à l'enregistrement utilisateur
- Domaine de l'utilisateur qui les crée

Le système empêche les tables suivantes d'être séparées par domaine :

- Contrôle d'accès [sys_security_acl]
- Script include [sys_script_include]
- Propriété système [sys_properties]
- Entités de la liste d'exclusion/d'inclusion de sécurité [sys_security_restricted_list]
- Entrée du dictionnaire [sys_dictionary]
- Contournement d'entrée de dictionnaire [sys_dictionary_override]

Affectation d'utilisateurs à des sociétés

Les administrateurs peuvent rapidement affecter des utilisateurs à un domaine en les affectant à une entreprise. Une fois que les utilisateurs sont affectés à un domaine, les enregistrements héritent automatiquement du domaine de l'utilisateur.

Par exemple, l'affectation de Bow Ruggeri à la société ACME l'affecte automatiquement au domaine ACME. L'affectation de Don Goodliffe à la société Initech l'affecte automatiquement au domaine Initech. Tous les enregistrements qu'ils créent sont automatiquement ajoutés au domaine approprié.

Utilisation de règles métier pour affecter des domaines

Les administrateurs peuvent utiliser une règle métier pour définir automatiquement une valeur de domaine lors de la création d'un enregistrement. La règle métier doit définir une valeur dans le champ **sys_domain** . Les administrateurs doivent s'assurer qu'il existe une colonne **sys_domain** disponible pour la table de l'enregistrement. Pour en savoir plus,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reportez-vous à la section Pratiques recommandées de séparation de domaine pour les fournisseurs de services.

Utilisation de modules pour affecter des domaines

Les administrateurs peuvent utiliser le paramètre **sysparm_domain** URL pour affecter automatiquement de nouveaux enregistrements à un domaine particulier à partir d'un module. Les administrateurs doivent créer un module avec une valeur **d'argument** : `sysparm_domain=sys_ID de domaine`.

Utilisation de modèles de formulaires pour affecter des domaines

Les administrateurs peuvent utiliser un modèle de formulaire pour affecter automatiquement de nouveaux enregistrements à un domaine particulier. Les administrateurs doivent ajouter le champ **sys_domain** au formulaire et sélectionner une valeur de domaine. Par exemple, si vous définissez le champ **sys_domain** sur **le domaine TOP/ACME** , tous les enregistrements de ce modèle sont automatiquement affectés au domaine TOP/ACME.

Héritage de domaine sur les tables

Par défaut, les enregistrements connexes héritent du domaine de l'enregistrement parent. Par exemple :

- Un enregistrement de tâche de changement hérite du domaine de l'enregistrement de demande de changement parent.
- Un enregistrement de problème hérite du domaine de l'enregistrement d'incident parent.

Affectation automatique de domaines basée sur les domaines d'utilisateur

Si aucune autre condition de domaine ne s'applique, un enregistrement hérite automatiquement du domaine de l'utilisateur qui le crée.

Domaines de visibilité et domaines contient

Les domaines de visibilité contrôlent ce qu'un utilisateur ou un groupe d'utilisateurs spécifique peut voir. Les domaines « contient » contrôlent ce qu'un domaine entier d'utilisateurs peut voir.

Domaines de visibilité

L'élément « Domaines de visibilité » détermine si les utilisateurs d'un domaine peuvent accéder aux enregistrements d'un autre domaine. Associez cet élément aux enregistrements d'utilisateur [sys_user] et de groupe [sys_user_group] dans les listes connexes de ces enregistrements. Les groupes accordent à leurs membres les domaines de visibilité du groupe. Lorsqu'un utilisateur quitte un groupe, il perd les domaines de visibilité du groupe. Accorder aux utilisateurs un domaine de visibilité accorde tous les droits sur les enregistrements de ce domaine en fonction des règles ACL (liste de contrôle d'accès).

Un domaine de visibilité :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Il s'agit d'une relation d'utilisateur à domaine explicitement accordée.
- N'est pas un domaine enfant.
- N'est pas contrôlé par la sélection dans le sélecteur de domaine. Les utilisateurs ayant accès à un domaine de visibilité voient toujours les données de ce domaine et de ses domaines enfants.

Remarque :
Il n'est pas recommandé d'utiliser les domaines de visibilité de manière excessive. Bien que la visibilité soit une méthode permettant aux utilisateurs d'accéder aux enregistrements, il est préférable d'utiliser des domaines contenant pour un contrôle plus robuste.

Contient des domaines

Normalement, les relations parent-enfant définissent la hiérarchie du domaine. Un domaine contient vous permet de relier des domaines selon vos besoins, indépendamment des relations parent-enfant. Toutefois, les domaines contiennent n'accordent de visibilité qu'aux données de domaine. Les processus ne sont pas affectés par les relations conteneur.

A contient le domaine :

- Est une relation plusieurs-à-plusieurs et de domaine à domaine.
- Peut avoir des domaines enfants. Lorsqu'un domaine est sélectionné, vous pouvez voir les données de ce domaine et de ses enfants.
- Est contrôlé par la sélection dans le sélecteur de domaine.

Remarque :
Lorsque vous ouvrez l'enregistrement de domaine, le champ d'application est défini sur le domaine de cet enregistrement, de sorte que vous ne pouvez voir que les domaines enfants. Choisissez **Activer/désactiver le champ d'application de domaine** dans le menu pour remplir la liste connexe.

Contient l'exemple de domaine

Lorsque le domaine d'accueil d'un utilisateur est A et que le domaine A contient les domaines B et C, ils deviennent tous des domaines pairs. Cela signifie que l'utilisateur voit les données des domaines A, B et C lorsqu'il se trouve dans son domaine d'accueil A. Si les utilisateurs changent de domaine avec le sélecteur de domaine pour le domaine B, ils ne voient que les données du domaine B. Lorsque les utilisateurs interagissent directement avec un enregistrement du domaine B ou du domaine C, ils ne voient que les données de ce domaine.

Exemple de domaine de visibilité

Avec la visibilité de domaine, si Don Goodliffe est dans le domaine Base de données, Bow Ruggeri est dans le domaine Réseau et qu'aucun incident n'est dans le domaine global, Don ne peut pas accéder aux incidents de Bow en raison de la séparation des données.

Hériter des domaines de visibilité en fonction de l'appartenance au groupe

Si vous définissez la table de domaine sur la table Groupe [sys_user_group], les utilisateurs peuvent hériter de domaines de visibilité en fonction de leur appartenance au groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Contient des requêtes et l’accès au domaine

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Champ d'application de domaine

Le champ d’application de domaine définit ce à quoi les utilisateurs peuvent et ne peuvent pas accéder.

Chaque utilisateur dispose de deux champs d’application de domaine lors de l’établissement d’une session dans une instance séparée par domaine.

- *Le champ d’application* de la session est défini lors de l’établissement de la session dans le domaine répertorié dans l’enregistrement utilisateur de l’utilisateur. Les utilisateurs peuvent modifier manuellement le champ d’application de leur domaine de session à partir du sélecteur de domaine.
- *Le champ d’application de l’enregistrement* utilise le domaine de l’enregistrement et est actif lors de l’affichage du formulaire de n’importe quel enregistrement.

Par défaut, le champ d’application de l’enregistrement a priorité sur le champ d’application de la session afin que les utilisateurs des domaines de niveau supérieur respectent les contraintes de données et de processus de chaque enregistrement. Toutefois, ces utilisateurs peuvent choisir d’étendre ou de réduire le champ d’application de domaine pour afficher ou masquer les données d’autres domaines. Par exemple, un utilisateur dans le domaine Fournisseur de service (SP) a également une visibilité sur les domaines enfants tels que le domaine ACME. Lorsqu’il examine un enregistrement d’incident à partir du domaine ACME, l’utilisateur peut choisir d’élargir le champ d’application de domaine pour afficher les valeurs du domaine SP ou de réduire le champ d’application de domaine pour afficher uniquement les valeurs d’enregistrement qui correspondent au domaine ACME de l’enregistrement.

Remarque :
Les utilisateurs ont toujours accès aux données des domaines qui leur ont été explicitement accordés par la visibilité du domaine.

Les utilisateurs disposant du rôle d’utilisateur domain_expand_scope peuvent sélectionner le champ d’application de domaine à partir de l’action d’interface utilisateur **Basculer le champ d’application de domaine** du formulaire. Lorsque le champ d’application de l’enregistrement est activé, cliquez sur l’action d’interface utilisateur pour le développer jusqu’au champ d’application de la session et afficher toutes les données disponibles en fonction du domaine de l’utilisateur et des domaines enfants. Lorsque le champ d’application de la session est activé, cliquez sur l’action d’interface utilisateur pour le réduire au champ d’application de l’enregistrement et afficher uniquement les données qui correspondent au domaine de l’enregistrement actuel.

Remarque :
Un enregistrement n’affiche pas l’action d’interface utilisateur permettant d’activer/de désactiver le champ d’application de domaine si l’enregistrement se trouve dans le domaine global ou si le domaine de l’utilisateur correspond au domaine de l’enregistrement.

Sélection de valeur d’enregistrement à partir d’autres domaines

Les utilisateurs qui peuvent voir plusieurs domaines ont la possibilité de sélectionner des valeurs d’enregistrement dans un domaine différent du domaine de l’enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, les agents Service Desk travaillant pour un fournisseur de service peuvent vouloir s'affecter certains incidents pour résoudre des problèmes au nom de leurs clients. Dans ce cas, le champ **Affecté à** de l'incident peut contenir un utilisateur du domaine SP, même si l'enregistrement d'incident lui-même est associé à un domaine enfant tel qu'ACME.

La sélection d'une valeur d'enregistrement d'un autre domaine ne modifie pas le domaine de l'enregistrement. L'enregistrement conserve son domaine d'origine. Lorsqu'un utilisateur consulte un enregistrement avec des valeurs de plusieurs domaines, la visibilité du domaine de l'utilisateur détermine ce qu'il voit.

Sélection de la valeur d'enregistrement

Lorsque ces conditions sont remplies	L'utilisateur a accès à ces éléments d'interface utilisateur
L'utilisateur a accès au domaine de l'enregistrement actuel référencé dans un champ.	L'utilisateur peut : • Voir la valeur d'affichage du champ de référence. Par exemple, le nom d'utilisateur est affiché dans le champ **Affecté à** . • Consultez l'enregistrement connexe à partir de l'icône de référence. Par exemple, l'enregistrement de l'utilisateur s'affiche dans le champ **Affecté à** . • Sélectionnez les valeurs de n'importe quel domaine visible. Par exemple, vous pouvez sélectionner des utilisateurs dans les domaines SP et ACME.
L'utilisateur n'a pas accès au domaine de l'enregistrement actuel référencé dans un champ.	L'utilisateur peut : • Ne pas voir les valeurs d'affichage du champ de référence. (C'est le cas si Séparation de domaine a été activée dans Madrid ou des versions ultérieures et que l'utilisateur n'a pas accès au domaine de cet enregistrement.) • Sélectionnez uniquement les valeurs du domaine de l'enregistrement. Par exemple, vous ne pouvez sélectionner que des utilisateurs à partir du domaine ACME.

Domaines et sociétés associées

Avec Séparation de domaine, vous pouvez transférer les modifications que vous apportez à un enregistrement de société au domaine et à d'autres enregistrements associés à la société.

Par défaut, le système affecte automatiquement les utilisateurs au même domaine que leur entreprise. Par exemple, tous les utilisateurs de la société ACME deviennent automatiquement membres du domaine TOP/ACME.

Remarque :
Les utilisateurs disposant du rôle admin peuvent modifier leurs propres enregistrements utilisateur et donc changer de domaine. Les fournisseurs de services peuvent désactiver l'administration déléguée ou configurer un processus d'approbation pour vérifier que l'utilisateur a besoin du rôle administrateur.

Lorsque vous changez le domaine d'une entreprise, l'instance change automatiquement le domaine des enregistrements associés suivants pour qu'il corresponde au nouveau domaine de l'entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Emplacements
- Départements
- Groupes
- Utilisateurs

Remarque :
L'instance ne change pas automatiquement le domaine des enregistrements pour lesquels vous avez coché la case **Domaine géré** .

Désactivation de domaine et sociétés associées

Lorsque vous désactivez un domaine, l'instance effectue automatiquement les actions suivantes.

- Désactive toutes les sociétés du domaine.
- Empêche tous les utilisateurs affectés à la société inactive de se connecter.

Remarque :
Lorsqu'un utilisateur d'une entreprise inactive tente de se connecter, il voit un message d'erreur similaire à Société inactive : votre accès à cette instance n'est pas autorisé.

Par exemple, si vous désactivez le domaine ACME à partir des exemples de données, l'instance désactive également la société ACME et les trois utilisateurs de l'échantillon sont verrouillés.

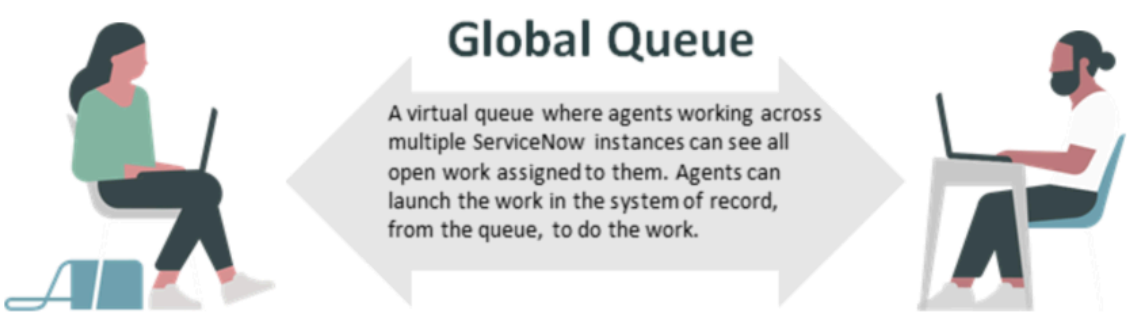
Concepts pour les fournisseurs de services

Ces concepts fonctionnent avec les options de la plateforme existante ServiceNow pour vous aider à résoudre les cas d'utilisation courants.

File d'attente globale v.2

Le concept de file d'attente globale fournit une vue virtuelle unique des tâches qui résident dans plusieurs instances. Le concept crée une application personnalisée pour fournir une vue de prestataire du travail qui réside dans plusieurs instances sans avoir à répliquer les tâches ou les données.

Vue d'ensemble



Les fournisseurs de services dont les agents travaillent sur des tâches provenant de plusieurs systèmes ont tendance à intégrer les données à une instance centrale, ou à une « chaise pivotante » entre les instances. Bien que cette méthode puisse être appropriée dans certains cas, elle peut être coûteuse et longue à construire et à entretenir. Cette méthode

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ouvre également le fournisseur à des considérations potentielles d'audit et d'exigence de données, telles que le Règlement général sur la protection des données (RGPD), dans tous les cas où les données se trouvent actuellement.

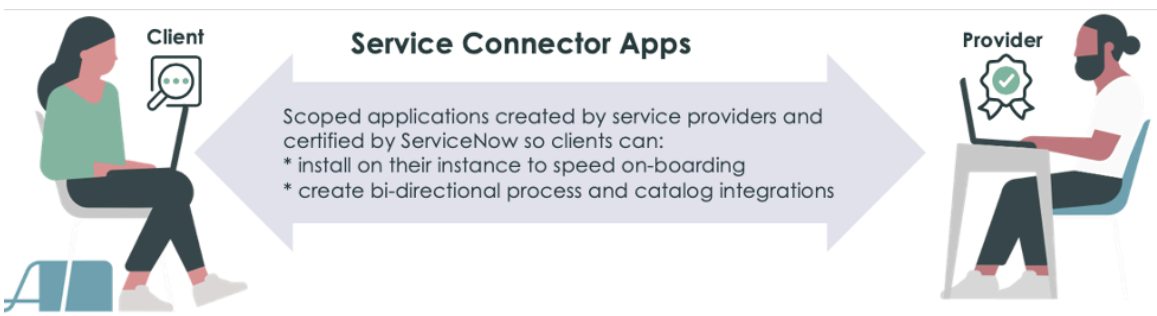
La file d'attente globale v.2 est une alternative : avec cette méthode, les agents peuvent voir les données qui leur sont affectées à partir d'une seule instance sans que les données souveraines ne persistent sur l'instance à laquelle ils sont connectés. Par exemple, dans les cas où les clients ont des exigences en matière de résidence des données, mais autorisent l'accès à des agents d'autres pays, le fournisseur peut utiliser un service d'assistance « follow the sun » utilisant la file d'attente globale v.2.

Pour en savoir plus sur la preuve de concept Global Queue v.2 , consultez le site Knowledge ServiceNow .

Remarque :
Dans la version Quebec, la preuve de concept de la file d'attente globale a été mise à niveau vers la file d'attente globale v. 2.

Connecteur fournisseur de service

L'application Service Provider Connector est une conception de référence pour la création d'une ServiceNow application Store que vos clients peuvent utiliser pour l'intégrer à vos systèmes. Les applications des fournisseurs de services vous aident à accélérer l'intégration et à créer des intégrations standardisées.



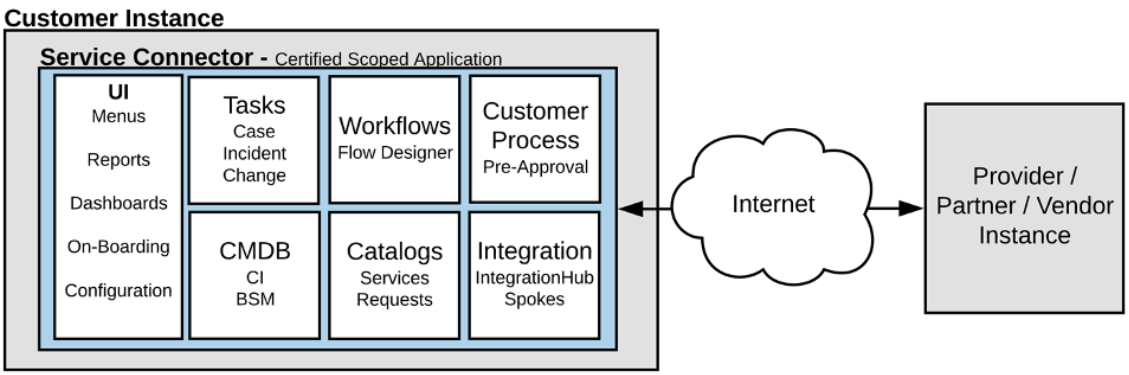
Avantages des connecteurs de service

Lorsque les fournisseurs de services (fournisseurs, partenaires) publient des connecteurs, l'intégration des clients est plus rapide, ce qui signifie une facturation plus rapide. Les instances intégrées augmentent la productivité, une plus grande visibilité dans l'écosystème et les avantages du ServiceNow programme de partenariat. Les avantages spécifiques sont les suivants :

- Élimine les intégrations personnalisées, y compris le coût des services nécessaires à leur livraison et à leur maintenance.
- Les services sont définis par le fournisseur au sein de leurs ServiceNow instances et éliminent la complexité et le coût des intégrations personnalisées.
- Les flux de travail et les demandes du catalogue peuvent être synchronisés, les processus et les approbations du client précédant les processus du fournisseur, afin que les clients puissent suivre leurs propres processus.
- Toutes les données créées ou modifiées (par exemple, les CI) pour le client sur l'instance du fournisseur peuvent être resynchronisées dans l'instance du client pour leur visibilité et leur utilisation dans les processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Fonctionnalités principales

Fonctionnalité	Description
Interface utilisateur	Un connecteur de service doit inclure au minimum les composants d'interface utilisateur suivants : • Rapports/tableaux de bord : les rapports et les tableaux de bord prédéfinis par profil aident à la visibilité. • Menu et modules – Le client doit être en mesure de trouver l'application via le fournisseur de menu descriptif **XYZ Services**. • Rôles : chaque connecteur nécessite des rôles d'utilisateur et d'administrateur pour garantir que l'accès peut être contrôlé par le client. Par exemple, « x_snc_xyz_user » ou « x_snc_xyz_admin ». • Intégration : une intégration rapide est essentielle à une bonne expérience client et doit être incluse via un playbook, une configuration guidée ou un élément de catalogue de sorte qu'aucun service professionnel ne soit requis pour la mise en service du client. (Des services professionnels sont disponibles, mais l'intégration peut être réalisée sans cela). • Configuration – Les points de données doivent être intégrés aux processus pour tenir compte de la majeure partie de la configuration normale du processus qu'un client doit réaliser. Cela élimine autant que possible les services professionnels. • Documentation – Une documentation complète augmente la satisfaction des clients et la facilité d'utilisation. • Intégration du support ou informations de contact – Le client a besoin d'un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	moyen simple de rester en contact avec le fournisseur de services pour tout problème, question ou demande.
Tâches	Utilisez l’application pour les tâches, telles que les incidents, les tickets, les changements, les problèmes, et ainsi de suite, qui doivent être prédéfinies dans le connecteur. Ces intégrations sont conçues pour garantir Studio de workflowCentre d'intégration le plus haut niveau de résilience et de performance.
CMDB	La synchronisation des données de base, telles que les CI requis pour les processus ITIL appropriés, doit être synchronisée entre les instances fournisseur et client.
Workflows	Tous les workflows doivent être conçus de Studio de workflow manière à garantir la résilience et les performances.
Catalogues	Le catalogue du fournisseur sollicité par le client doit être inclus dans l’application en tant que catalogue producteur d’enregistrements. La demande générée par l’élément dans l’instance du client doit être liée électroniquement aux instances du fournisseur. Les workflows du fournisseur maintiennent la demande à jour et la resynchronisent vers l’instance du client.
Processus client	Tout mécanisme de synchronisation des demandes avec l’instance du fournisseur doit permettre aux processus clients d’interagir avec les demandes avant qu’elles ne soient envoyées à l’instance du fournisseur. Pendant le traitement du fournisseur, les approbations peuvent être envoyées à l’instance du client selon les besoins.
Intégration	Les intégrations doivent être créées en utilisant Studio de workflow et Centre d'intégration pour garantir le plus haut niveau de résilience et de performance.

Composants que vous pouvez inclure dans un connecteur de service

Composant	Description
Réplication de données d’instance (IDR)	Lorsque la réplication est l’objectif : • Peut être utilisé pour l’intégration de processus, mais peut être trop rigide en fonction de la complexité Logique d’intégration basée sur la transition d’état • Pour en savoir plus, consultez Réplication de données d’instance
Centre d'intégration	Lorsque l’intégration des processus est l’objectif :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composant	Description
	• Plus facile à injecter au milieu d'un processus, dans le cadre d'une étape complexe ou conditionnelle au milieu d'un flux • Pour plus d'informations, consultez Centre d'intégration
File d'attente de travail globale (virtuelle)	Lorsque l'objectif est la fédération de tâches et que le stockage des données en externe n'est pas acceptable : • Utilisé lorsque les agents travaillent sur plusieurs ServiceNow instances et ont besoin de voir tout le travail ouvert qui leur est affecté • Les lignes renvoyées doivent être limitées à moins de 1 000 • Pour en savoir plus, voir File d'attente de travail globale
Tables distantes	Lorsque l'objectif est l'utilisation de données externes sans stockage : • Utilisé pour connecter une instance à des sources tierces, ou à une autre instance, pour récupérer des données externes et éventuellement les mettre en cache dans la mémoire. Les données sont traitées comme une table dans l'instance à des fins de lecture seule telles que regroupement, tri, agrégation et filtre. • Pour en savoir plus, consultez Récupération de données externes à l'aide de tables et de scripts distants
Concepteur de flux	Lorsque la conception des processus est l'objectif • Permet d'automatiser les processus dans un environnement de conception unique. Les propriétaires de processus peuvent utiliser le langage naturel pour automatiser les approbations, les tâches, les notifications et les opérations d'enregistrement sans codage. • Pour en savoir plus, reportez-vous à la rubrique Flow Designer .

Pour en savoir plus sur la preuve de concept de Service Connector , consultez le site de la ServiceNow base de connaissances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants installés avec Séparation de domaine

Plusieurs composants de la plateforme sont ajoutés ou modifiés avec Séparation de domaine.

Rôles

Rôle	Description
domain_admin	Peut créer, modifier et supprimer des domaines.

Ajouts aux champs [sys_domain]

Le champ sys_domain est ajouté aux tables suivantes :

Tables avec le champ sys_domain

Tables
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_gauge
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

Champ pour la table de tâches

Les extensions MSP ajoutent un champ task_for à la table Tâche. Ce champ de référence fait référence à la table Utilisateur.

Options pour le type de groupe

Les extensions MSP ajoutent plusieurs nouvelles options par défaut au champ Type de la table Groupe. Ajoutez ou mettez à jour ces types selon vos besoins pour prendre en charge vos domaines.

Tables
Sécurité
Prise en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables
Visibilité

Règles métier

Nom	Table	Description
Domaine : activer/ désactiver	core_company	Active le domaine connexe si au moins une de ses sociétés est active. Désactive le domaine connexe si toutes les sociétés liées sont inactives.
Domaine : société en cascade	core_company	Synchronise le domaine d'une entreprise avec ses utilisateurs, groupes, départements et emplacements.
Domaine : domaine en cascade : e-mail	sys_email	Synchronise le domaine d'un e-mail avec ses pièces jointes.
Domaine : cascade Domaine : groupe	sys_user_group	Synchronise le domaine d'un groupe avec ses rôles hérités (enregistrements sys_group_has_role).
Domaine : domaine en cascade : Knowledge	kb_knowledge	Synchronise le domaine d'un article de la base de connaissances avec ses commentaires connexes.
Domaine : domaine en cascade : tâche	tâche	Synchronise le domaine avec les tâches connexes pour wf_context, wf_executing, wf_history, pièces jointes, e-mails, task_sla et son workflow, sysapproval_approver et son workflow, et sysapproval_group et son workflow.
Domaine : domaine en cascade : utilisateur	sys_user	Synchronise le domaine d'un utilisateur avec ses enregistrements d'appartenance au groupe (sys_user_grmember) et de rôle (sys_user_has_role).
Domaine : domaine en cascade : version	wf_workflow_version	Synchronise les domaines avec les versions de workflow connexes pour les wf_activity et les wf_transition.
Domaine : désactiver les sociétés	domain	Désactive les sociétés associées si un domaine est désactivé.
Domaine : Par défaut : Tâche	tâche	Définit le domaine de tâche en fonction de la tâche pour le domaine de l'utilisateur. Si ce domaine est global, définit plutôt le domaine sur Par défaut.
Domaine : Par défaut : Utilisateur	sys_user	Définit le domaine d'un utilisateur sur la valeur par défaut si le domaine aurait autrement été global.
Domaine : interdire l'enregistrement	domain	Empêche la création d'un domaine avec le nom global.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
de domaine global		
Domaine : remplacer la copie	sys_app_application	Lorsqu'une application est remplacée par un domaine, crée une copie de ses modules pour la nouvelle application.
Domaine : remplacer la copie	sys_data_policy2	Lorsqu'une politique de données est remplacée pour un domaine, crée une copie de ses règles de politique de données pour la nouvelle politique de données.
Domaine : remplacer la copie	sys_gauge	Lorsqu'une jauge est remplacée pour un domaine, crée une copie de son nombre de jauges pour la nouvelle jauge.
Domaine : remplacer la copie	sys_ui_action	Lorsqu'une action d'interface utilisateur est remplacée pour un domaine, crée une copie de ses vues d'action d'interface utilisateur pour la nouvelle action d'interface utilisateur.
Domaine : remplacer la copie	sys_ui_list_control_embedded	Lorsqu'un contrôle de liste incorporé est remplacé pour un domaine, crée une copie de ses scripts client et serveur pour le nouveau contrôle de liste incorporé.
Domaine : remplacer la copie	sys_ui_policy	Lorsqu'une politique d'interface utilisateur est remplacée pour un domaine, crée une copie de ses actions de politique d'interface utilisateur pour la nouvelle politique d'interface utilisateur.
Domaine : Définir Domaine : Approbations	sysapproval_approver	Définit le domaine en fonction de celui de l'enregistrement en cours d'approbation.
Domaine : définir Domaine : pièce jointe	sys_attachment	Définit le domaine en fonction du domaine de l'enregistrement parent.
Domaine : défini Domaine : CMDB_CI	cmdb_ci	Définit le domaine d'un CI sur celui de sa société.
Domaine : Définir Domaine : Département	cmn_department	Définit le domaine d'un département sur celui de sa société.
Domaine : définir Domaine : domaine	domain	Définit le domaine d'un domaine en lui-même.
Domaine : définir Domaine : E-mail	sys_email	Définit le domaine en fonction du domaine de l'enregistrement parent. L'enregistrement parent d'un e-mail est l'enregistrement spécifié dans le champ d'instance.
Domaine : Définir	kb_feedback	Définit le domaine d'un commentaire de la base de connaissances sur celui de son article de la base de connaissances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
Domaine : Commentaire		
Domaine : Définir Domaine : Groupe	sys_user_group	Définit le domaine d'un groupe sur celui de sa société.
Domaine : Définir Domaine : Approbations de groupe	sysapproval_group	Définit le domaine en fonction de celui de l'enregistrement en cours d'approbation.
Domaine : Définir Domaine : Rôle du groupe	sys_group_has_role	Définit le domaine d'un rôle de groupe sur celui de son groupe.
Domaine : Définir Domaine : Emplacement	cmn_location	Définit le domaine d'un emplacement sur celui de son entreprise.
Domaine : Définir Domaine : SLA de tâche	task_sla	Définit le domaine d'un SLA de tâche sur celui de sa tâche.
Domaine : Définir Domaine : Utilisateur	sys_user	Définit le domaine d'un utilisateur sur celui de sa société.
Domaine : Définir Domaine : Rôle de l'utilisateur	sys_user_has_role	Définit le domaine d'un rôle d'utilisateur sur celui de son utilisateur.
Domaine : définir Domaine : Historique des activités WF	wf_history	Définit le domaine d'historique de l'activité du workflow en fonction du domaine du contexte de workflow parent.
Domaine : définir Domaine : contexte WF	wf_context	Définit le domaine du contexte du workflow en fonction du domaine de l'enregistrement référencé, le cas échéant.
Domaine : Définir Domaine : Activité d'exécution WF	wf_executing	Définit le domaine de l'activité d'exécution du workflow en fonction du domaine du contexte de workflow parent.
Domaine - Définir la tâche pour - Changement	demande de changement	Lors de la conversion d'un ticket en demande de changement, définit le champ Demandé par sur la tâche du ticket pour la valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
Domaine - Définir la tâche pour - Incident	incident	Lors de la conversion d'un ticket en incident, définit le champ Appelant sur la tâche du ticket pour la valeur.
Domaine : valider la valeur par défaut	domain	Garantit que la case Par défaut est cochée pour un seul domaine.
Domaine : valider le primaire	domain	Garantit que la case Primaire est cochée pour un seul domaine.
Règles métier installées avec le module d'extension Domain Support		
Modifier l'ensemble de domaines	sys_dictionary	Définit l'ensemble de domaines sur le domaine actuel.
Propriétés de prise en charge du domaine	sys_properties	Définit les propriétés système pour qu'elles correspondent à la méthode de requête de domaine (chemins de domaine ou numérotation des domaines).

Scripts clients

Script client	Description
Domaine : définir la société et l'emplacement (sys_script)	Surveille le champ de l'appelant de l'incident pour connaître les changements. Si les champs Société et Emplacement n'ont pas déjà de valeur, le script ajoute ces informations à partir de l'enregistrement de l'appelant. Si les champs Société et Emplacement ont déjà une valeur, le script conserve les valeurs existantes.
Script désactivé	
(BP) Définir l'emplacement sur l'utilisateur	Surveille le champ d'emplacement de l'incident et définit le champ d'emplacement sur l'emplacement de l'appelant.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Prise en charge des applications pour Domain Separation

De nombreuses applications prennent en charge Séparation de ServiceNow domaine dans le système de base, mais pas toutes. Certaines applications prises en charge incluent des limitations sur les données et les paramètres administratifs qui peuvent être séparés par domaine. Ces définitions définissent les niveaux de prise en charge de Séparation de domaine du point de vue des cas d'utilisation réels et des personnes qui les utilisent.

Niveaux de prise en charge de Domain Separation

ServiceNow Les applications qui prennent en charge Séparation de domaine peuvent uniquement prendre en charge la séparation des données et l'acheminement des données, disposer d'une séparation de logique métier avancée ou prendre en charge l'administration de l'application au niveau du locataire (client). ServiceNow Les applications sont définies avec les niveaux de prise en charge incrémentielle suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Aucune prise en charge

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Élémentaire

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de services (SP) de l'application.
- Dans l'application, l'interface utilisateur, les clés de cache, les rapports, les déploiements, les agrégations et autres utilisent tous un domaine au moment de l'exécution de la production.
- Le propriétaire de l'instance doit pouvoir configurer l'application pour qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un SP utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir voir la réponse du SP.

Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : les processus peuvent être créés ou modifiés par client par le fournisseur de services (SP). Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de rendre les commentaires obligatoires lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Amélioré

- Inclut les niveaux **Basique** et **Standard**.
- Le processus piloté par les données permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas en affecter une autre.

- Les locataires de l'instance doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) pour eux-mêmes. Cette logique et ces paramètres sont attendus pour un fonctionnement normal de l'application.

Exemple de cas d'utilisation : les locataire-clients d'un environnement partagé doivent pouvoir passer à la matrice d'impact, d'urgence ou de priorité pour définir la priorité au sein de leur domaine.

Remarque :
Domaine effectif (*)

Parfois, une fonctionnalité ou une application de plateforme peut prendre en charge efficacement les cas d'utilisation SP même sans le cadre de travail de domaine. Si tel est le cas, les cas d'utilisation doivent détailler sa prise en charge de Domain Separation. Un astérisque (*) après le niveau de prise en charge indique ce type de configuration.

Fonctionnalité prise en charge	Élémentaire	Standard	Amélioré
La colonne Domaine est présente pour les tables d'application du système de base.	●	●	●
La configuration spécifique à un domaine est gérée par le propriétaire de l'instance.	●	●	●
Les domaines de locataire peuvent gérer leurs propres données d'application.		●	●
Les propriétés de l'application sont sensibles au domaine en cas de besoin.		●	●
Les processus et la logique métier peuvent être séparés par domaine par le propriétaire de l'instance.		●	●
La logique et les processus métier peuvent être administrés par le domaine du locataire.			●

Niveaux de prise en charge par application

Suite de produits	Application	Niveau de prise en charge
App development and low-code	App Engine Studio	Aucune prise en charge
	Automation Center	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Concentrateur de l'automatisation des processus robotiques (RPA)	Élémentaire
	ServiceNow Studio	Aucune prise en charge
	Générateur de tables	Élémentaire
	App Engine Management Center	Aucune prise en charge
	Exploring Decision Tables	Standard
	Intégration de la planification des ressources de l'entreprise	Aucune prise en charge
	Planification des ressources de l'entreprise Exploration de la personnalisation	Aucune prise en charge
	Générateur d'IU Next Experience	Élémentaire
Gestion du service clientèle	Communities	Aucune prise en charge
	Gestion du service clientèle	Élémentaire
	Gestion des mises en production	Basique*
	Order Management pour Customer Service Management	Élémentaire
	Support après-vente	Élémentaire
	Domain separation in Workforce Optimization for Customer Service	Élémentaire
DevOps	Domain separation and DevOps Change Velocity	Aucune prise en charge
	Domain separation and DevOps Config	
Gestion des services aux employés	HR Service Delivery	Basique*
	Santé et sécurité	Aucune prise en charge
	Contract Management Pro	Élémentaire
	Legal Service Delivery	Élémentaire
	Gestion des services de procurement (PSM)	Aucune prise en charge
	Suite Lieu de travail sécuritaire	Consultez le site de l'application pour les niveaux de prise en charge des applications individuelles
	Connecteur de recherche SharePoint Online	Élémentaire
	Demande universelle	Élémentaire
	Tâche universelle	Élémentaire
	Optimisation des effectifs pour RH	Élémentaire
Gestion environnementale, sociale et de gouvernance	Gestion environnementale, sociale et de gouvernance	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
Field Service Management	Field Service Management	Élémentaire
Gouvernance, risque et conformité	Business Continuity Management	Élémentaire
	Gouvernance, risque et conformité (GRC)	Élémentaire
	Operational Resilience	Élémentaire
Produits spécifiques à chaque secteur		
•Financial Services	Financial Services Card Operations	Élémentaire
	Financial Services Deposit Operations	
	Financial Services Payment Operations	
	Service intelligent pour la fraude	
	Gestion des services d'assurance de dommages	
	Gestion des services d'assurance-vie	
	Réclamations d'assurance	
	Financial Services Know Your Customer	
	Opération de crédit de services financiers	
	Processeur de document de services financiers	
• Santé et sciences de la vie	Support EMR	Élémentaire
	Santé et sciences de la vie Service Management Core	Élémentaire
	Pre-Visit Management	Élémentaire
	Patient Support Services	Élémentaire
	Vaccine Administration Management	Élémentaire
Activités commerciales de la fabrication	Activités commerciales de la fabrication	Standard
	Base de vente au détail	Élémentaire
	Gestion des tâches de vente au détail	Élémentaire
• Production industrielle	Industrial Process Manager	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Response	Standard
	Operational Technology Manager	Standard

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
Telecommunications, Media, and Technology (TMT)	Gestion de la réussite client	Élémentaire
	Gestion des problèmes du service clientèle	Élémentaire
	Now Assist for Telecommunications, Media and Technology (TMT)	Basique (hérité de Domain separation in the Now Assist Admin console).
	Proactive Service Experience Workflows	Standard
	Pont de services	Standard
	Product Support for Technology application	Basique (hérité de Gestion du service clientèle).
	Telecommunications Network Inventory	Élémentaire
Gestion des actifs IT	Cloud Insights	Aucune prise en charge
	Hardware Asset Management	Amélioré
	Gestion des actifs logiciels	Amélioré
	Enterprise Asset Management	Standard
Strategic Porfolio Management	Agile Development	Basique*
	Alignment Planner Workspace	Élémentaire
	Application Portfolio Management	Élémentaire
	Cost Management	Aucune prise en charge
	Gestion de la demande	Élémentaire
	Gestion financière	Aucune prise en charge
	Investment Funding	Élémentaire
	Project Portfolio Management	Basique*
	Gestion des mises en production	Basique*
	Scaled Agile Framework (SAFe)	Basique*
	Test Management	Basique*
	Cadre de travail des objectifs	Élémentaire
IT Operations Management	Cloud Provisioning and Governance	Élémentaire
	Agent Client Collector	Élémentaire
	Discovery	Standard
	Event Management	Élémentaire
	Espace de travail pour l'exploitation des services pour ITOM	Élémentaire
	Health Log Analytics	Élémentaire
	Analyse des mesures	Élémentaire
	Service Mapping	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Évaluation de la migration vers le cloud	Élémentaire
	Bibliothèque d'actions	Aucune prise en charge
	Cloud Configuration Governance	Aucune prise en charge
	Gouvernance des balises	Élémentaire
	Facturation d'Analyse des coûts du cloud	Aucune prise en charge
	Cloud Provisioning and Governance : Google Cloud	Élémentaire
	Cloud Provisioning and Governance Terraform	Élémentaire
	Espace de travail pour l'exploitation dans le cloud	Élémentaire
	Découverte dans le cloud	Standard
IT Service Management	Benchmarks	Aucune prise en charge
	Gestion des changements	Élémentaire
	Coaching	Élémentaire
	Gestion de l'amélioration continue	Élémentaire
	Gestion des contrats	Aucune prise en charge
	Domain separation and Digital Product Release	Élémentaire
	Ligne de dépense	Aucune prise en charge
	Incident Communications Management	Standard
	Gestion des incidents	Standard
	Facilities Service Management	Standard
	Gestion des incidents	Standard
	Planification d'astreinte	Standard
	Gestion des actifs	Élémentaire
	Problem Management	Standard
	Approvisionnement	Standard*
	Catalogue de produits	Standard
	Gestion des requêtes	Standard
	Catalogue de services	Standard
	Service Level Management	Élémentaire
	Gestion des portefeuilles de services	Basique*
	Opérations pour la fiabilité des sites	Basique*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Panne de tâche	Élémentaire
	Domain separation and Vendor Management Workspace	Aucune prise en charge
	Walk-up Experience	Élémentaire
Configuration et navigation Mobile	Mobile	Élémentaire
Now Intelligence	Tableaux de bord	Élémentaire
	Performance Analytics	Amélioré
	Process Optimization	Élémentaire
	Reporting	Élémentaire
	User Experience Analytics	Élémentaire
Le champ ServiceNow AI Platform	Administration	
	Domain separation and Agent Chat	Standard
	ServiceNow AI Platform Options	
	Interface utilisateur	
	Affectation de travail avancée	Standard
	AI Search	Les recherches respectent les restrictions de domaine des enregistrements indexés
	App Engine Studio	Aucune prise en charge
	Gestion des applications	Aucune prise en charge
	Évaluations	Standard
	Automated Test Framework	Standard*
	Fonctions vocales ServiceNow	
	Signature de code	Prise en charge de base
	Contextual Search	Standard
	Configuration Management (CMDB)	Standard
	Système de gestion du contenu	Aucune prise en charge
	Informations d'identification et connexions	Standard
	Certification des données	Basique*
	Classification des données	Amélioré
	Confidentialité des données	Aucune prise en charge
	Gestion des données	Basique*
	Développement délégué	Aucune prise en charge
	Dependency Views	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Services documentaires	Aucune prise en charge
	Dynamic Translation	Élémentaire
	Edge Encryption	Prise en charge de base
	Connecteurs de contenu externe	Aucun support*
	Chiffrement de champ	Aucune prise en charge
	Chiffrement	Aucune prise en charge
	Chiffrement dans le cloud avec gestion des clés	Prise en charge de base
	Normalisation de champ	Aucune prise en charge
	Flow Designer	Standard*
	Configuration guidée	Aucune prise en charge
	Domain separation and Integration Hub	Standard*
	Intégrations avec des applications et des sources de données tierces	Basique+Standard
	Knowledge Management	Standard
	Service de messagerie Hermes	Aucune prise en charge
	Documents gérés	Aucune prise en charge
	MetricBase	Élémentaire
	Compréhension de l'agriculture naturelle	Basique+Standard
	Notifications	Standard
	Pilote ODBC	Basique*
	Orchestration	Standard*
	Password Reset	Standard
	Sécurité de la plateforme	Page de destination Séparation de domaine
	Confidentialité des données	Aucune prise en charge
	Intelligence prédictive	Standard
	Déclencheurs proactifs	Élémentaire
	Process Automation Designer	Élémentaire
	Tables distantes	Aucune prise en charge
	Calendriers	Élémentaire
	Débogueur de script	Élémentaire
	Suggestions de recherche	Aucune prise en charge
	Service Portal	Aucune prise en charge
	Connecteurs du graphe de services	Aucune prise en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Domain separation and Sidebar	Standard
	Flux d'états	Aucune prise en charge
	Subscription Management	Basique*
	Gestion des enquêtes	Basique*
	Intelligence des tâches	Aucune prise en charge
	Domain separation and Time Card	Basique*
	UI Builder	Standard
	Agent virtuel	Élémentaire
	Visual Task Boards	Élémentaire
	Services Web	Standard*
	Workflow	Standard*
	Espace de travail	Standard
Security Operations	Configuration Compliance	Standard
	Gestion des données de configuration	Élémentaire
	IBM QRadar Offense Ingestion	Élémentaire
	Intégration de l'ingestion d'alertes de l'API Microsoft Graph Security	Élémentaire
	Security Incident Response	Standard
	Threat Intelligence	Standard
	Vulnerability Response	Standard
Service Management	Facilities Service Management	Standard
	Planned Maintenance	Standard*
	Déclencheurs proactifs	Élémentaire
	Éditeur de code NOW	Aucune prise en charge
	Optimisation des effectifs pour ITSM	Élémentaire
	Vendor Management Workspace	Élémentaire

Traduction automatique

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Vous pouvez créer, implémenter et gérer Séparation de domaine pour vos applications et services.

Bases du domaine

Avec Séparation de domaine (également connue sous le nom d'architecture ServiceNow de plateforme mutualisée), vous pouvez séparer les données d'application, l'interface utilisateur et la logique métier dans une instance client unique qui prend en charge la modélisation hiérarchique avec l'intelligence interlocataire. La logique métier décrit

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

comment la séparation de domaine est configurée et quelles règles affectent la configuration.

Avant de vous lancer dans l'aventure de séparation par domaine, voici quelques bonnes pratiques à suivre. Sélectionnez les rubriques comme vous le souhaitez ou suivez-les dans l'ordre en cliquant sur les liens sous l'image.



L'explication de Domain Separation

Avec Séparation de domaine, vous pouvez séparer les données d'application, l'interface utilisateur et la logique métier, comme les règles ou les workflows, dans une seule instance client. La séparation de ces éléments en domaines définis de manière logique prend en charge des hiérarchies spécifiques pour tous les clients qui utilisent vos applications.

Bases du domaine

Domain Separation, également connue sous le nom d'architecture ServiceNow de plateforme mutualisée, ajoute des frais généraux considérables à la gestion d'une instance. Cependant, si vous utilisez correctement Séparation de domaine, elle peut améliorer l'efficacité, renforcer la sécurité et augmenter les performances des instances de vos clients.

Vous ne pouvez pas séparer certaines normes et propriétés globales, telles que les propriétés système et le schéma de table, par locataire.

Avant de commencer à séparer des domaines, lisez les instructions suivantes.

Ce que vous pouvez faire avec Séparation de domaine

- Séparation des données : permet aux locataires du domaine de voir uniquement les données qu'ils ont l'autorisation de voir. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données de locataire auxquelles ils n'ont pas accès.

Traduction automatique

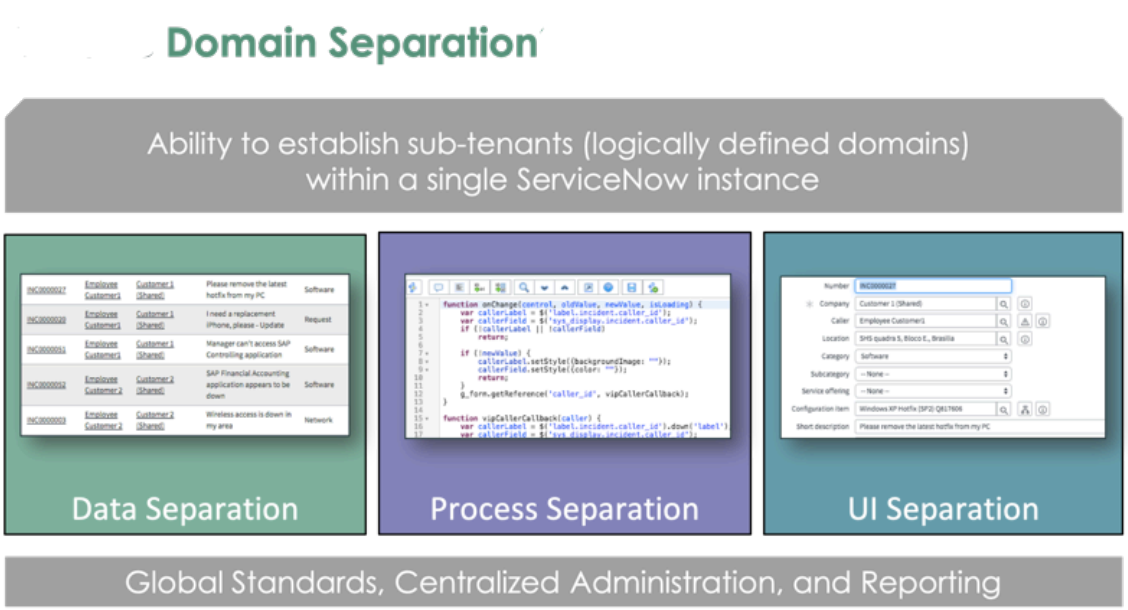
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsque vous mettez à jour des enregistrements de données, ils ne génèrent pas d'enregistrements d'ensembles de mises à jour.
- Les utilisateurs, y compris les comptes clients utilisés pour les intégrations, ne voient que les données des domaines auxquels ils ont l'autorisation d'accéder.
- Les clients, les agents et les prestataires voient les données relatives aux clients et aux organisations qu'ils assistent.

- Séparation de l'interface utilisateur : prend en charge une expérience spécifique au locataire pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.
  - Vous pouvez remplacer l'interface utilisateur basée sur un navigateur, y compris les menus d'application, les listes, les formulaires et les tableaux de bord. Vous pouvez également les personnaliser pour un domaine spécifique ou un ensemble de domaines tout en préservant votre logique de processus de base.
  - Les fournisseurs de services peuvent modifier les éléments de marque et d'interface utilisateur affichés pour répondre aux besoins individuels des clients.
- Séparation de la logique métier : crée des politiques système spécifiques au locataire, telles que les notifications par e-mail, les règles métier, les scripts clients, la politique d'interface utilisateur et les actions d'interface utilisateur.
- Modélisation hiérarchique : imbrique vos multiples locataires afin que les locataires parents puissent accéder aux ressources des locataires enfants. La logique métier pour les locataires parents s'exécute automatiquement pour les locataires enfants, que vous pouvez remplacer à n'importe quel niveau.
- Intelligence interlocataire : gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires ayant accès à des données de locataire supplémentaires.

Séparation de domaine en un coup d'œil

Le graphique suivant montre la division des données, le processus et la séparation de l'interface utilisateur. Ces concepts sont abordés en détail dans la section Pratiques recommandées.



Traduction automatique

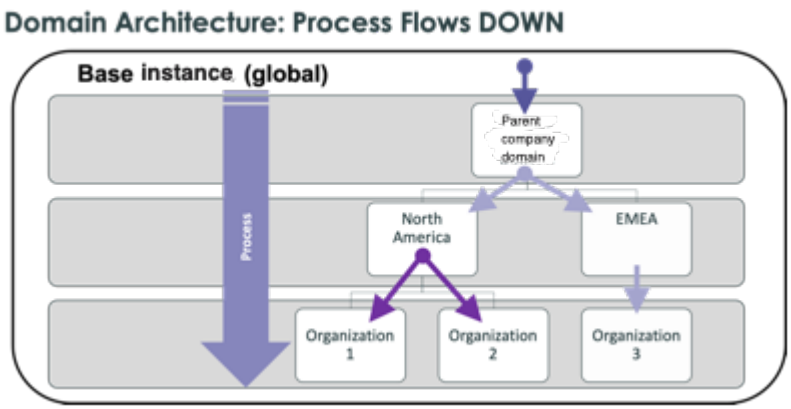
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture du domaine

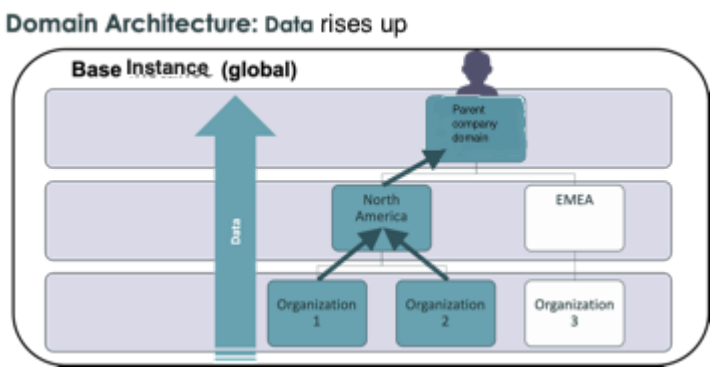
Les enregistrements utilisateur se voient attribuer une valeur de domaine qui représente le domaine d'accueil de l'utilisateur. Les utilisateurs n'ont pas accès aux données des domaines parents, des domaines homologues ou des domaines d'autres branches de la hiérarchie.

Consultez la section Contient des requêtes et l'accès au domaine pour les options avancées permettant d'accorder une visibilité supplémentaire sur le domaine.

Le diagramme suivant montre comment le processus d'architecture s'écoule vers les



domaines enfants.



Proposition de valeur de Domain Separation

Avec Séparation de domaine, les fournisseurs de services peuvent disposer d'une architecture d'instance mutualisée qui fournit des offres de manière efficace et sécurisée à leurs clients. Des normes de processus universelles solides, une conception de processus axée sur les données, une gouvernance stricte et une administration centralisée permettent de maximiser ces avantages.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantages de Domain Separation

Les locataires d'un domaine bénéficient d'un retour sur investissement rapide, de frais administratifs réduits et de l'exploitation des services d'entreprise fournis par les propriétaires d'instances.

Voici un aperçu rapide de ces avantages.

Propriétaire de l'instance	Locataires du domaine
Productivité des employés du fournisseur de service	Sécurité accrue
Seuls les deltas de processus maintenus	Processus et fonctionnalités prédéfinis
Efficacité de l'administration	Réduction du personnel requis
Moins d'intégrations client	Intégration plus rapide
Évolutivité et évolutivité	Exploitation des dernières versions
Ségrégation des données	Services fournis par le propriétaire de l'instance
Rapports globaux	

Définition de la séparation en domaines

Avec Séparation de domaine (également connue sous le nom d'architecture de plateforme mutualisée), vous pouvez séparer les données d'application, l'interface utilisateur et la logique métier dans une instance client unique qui prend en charge la modélisation hiérarchique avec l'intelligence ServiceNow® interlocataire (client).

Propriétés de la séparation en domaines

Les applications séparées par ServiceNow domaine sont définies avec les propriétés suivantes :

Séparation des données

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Permet aux clients de voir uniquement les données qu'ils sont autorisés à voir. Les clients peuvent avoir accès à d'autres données client, mais ne peuvent pas interroger les données client s'ils n'y ont pas accès.

Séparation de l'interface utilisateur

Prend en charge une expérience client spécifique pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.

Séparation de la logique métier

Prend en charge les politiques système spécifiques au client telles que les notifications par e-mail, les règles métier, les scripts clients, la politique d'interface utilisateur et les actions d'interface utilisateur.

Modélisation hiérarchique

Prend en charge la mutualisation imbriquée afin que les locataires parents (clients) puissent accéder aux ressources client enfants. La logique métier pour les clients parents s'exécute automatiquement pour les clients enfants et peut être remplacée à n'importe quel niveau.

Intelligence inter-clients (champ d'application de domaine)

Gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires qui ont accès à des données de locataire supplémentaires.

Hiérarchies Domain Separation

Créez une hiérarchie lorsque vous définissez une architecture de domaine afin de suivre vos processus et workflows.

Exemples de hiérarchies Domain Separation

Le diagramme suivant est un bon point de départ pour définir l'architecture de domaine. Il montre la relation entre les domaines TOP et inférieurs et comment le processus, les données et les règles métier ont un impact sur les domaines parent et enfant.

- Dans l'exemple suivant, TOP est un domaine de processus. Il ne doit jamais contenir d'utilisateurs. À la place, TOP doit contenir les nouveaux processus que les propriétaires d'instances développent et les remplacements vers ces processus à partir du domaine global.
- Seul le fournisseur de service (SP) a accès au domaine par défaut. Ce domaine ne contient jamais d'utilisateurs actifs. Il contient uniquement les données « perdues » que vous devez réaffecter au domaine approprié.

  Remarque :
  Lorsque les données ne sont pas affectées à un domaine spécifique, elles se déplacent vers le domaine par défaut. Elles sont alors temporairement « perdues » et doivent être affectées au domaine approprié.

- Les tâches et les utilisateurs sans domaine sont placés automatiquement dans le domaine par défaut lorsque vous créez ou mettez à jour des domaines. Vous pouvez remplacer cette action en effaçant l'option **Par défaut** sur cet enregistrement ou en sélectionnant l'option **Par défaut** sur un autre enregistrement de domaine. Si vous n'avez pas encore défini de domaine par défaut, les tâches et les utilisateurs sans domaine se déplacent vers le domaine global.
  - Ne déplacez pas les données entre les domaines lorsque vous utilisez l'instance.
  - Si des données finissent dans le domaine par défaut, cela signifie que vous avez un problème de configuration ou de procédure à résoudre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

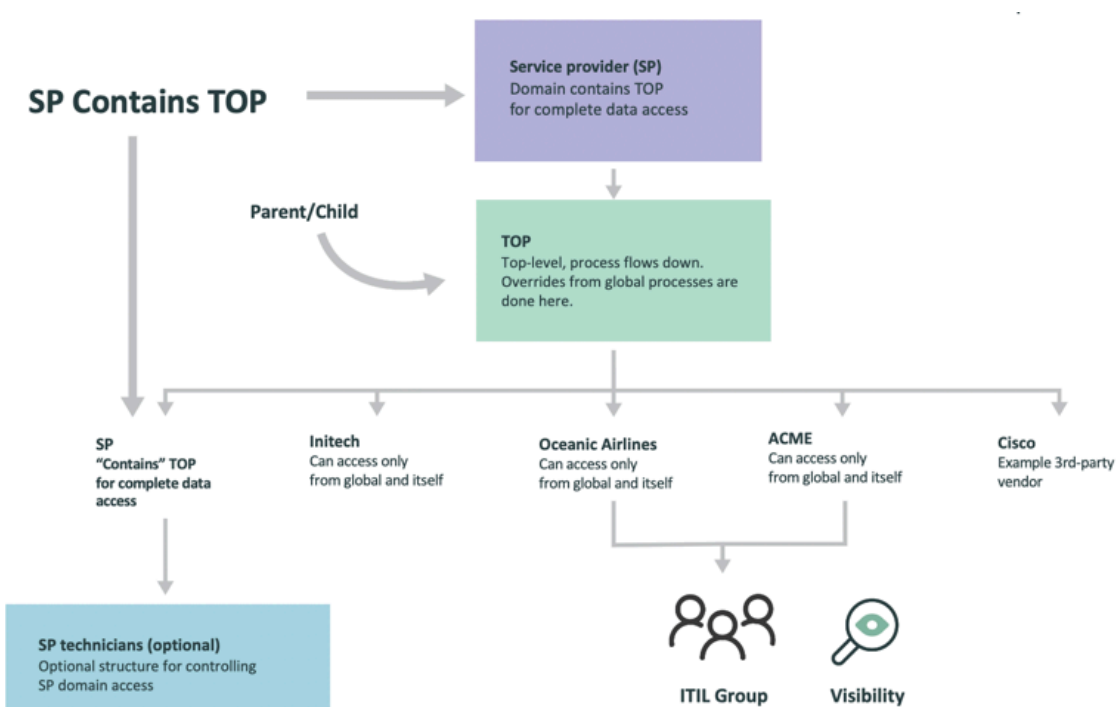
Vous ne voyez pas le mot « Global » dans ce diagramme car il n'y a pas de domaine global. N'oubliez pas que « global » se traduit par l'absence d'un domaine dans un enregistrement.

Par exemple, lorsqu'une table n'a aucun champ de domaine, cela signifie qu'elle contient tous les enregistrements globaux. Lorsqu'une table possède un champ de domaine, cela signifie que tout enregistrement sans domaine est un domaine global.

Le mot « global » se trouve dans le champ Domaine. Il y est placé automatiquement lorsque l'enregistrement n'a pas de domaine.

Les enregistrements globaux sont disponibles pour tous les utilisateurs de l'instance, sauf s'ils sont restreints par des configurations de sécurité.

- Utilisez le domaine par défaut pour vous assurer que les enregistrements ne finissent pas dans le domaine global sur des tables qui ne doivent jamais avoir d'enregistrements globaux.
- Les propriétaires d'instances doivent ensuite trier les enregistrements dans le domaine par défaut et les déplacer vers le domaine approprié.



Hiérarchies de domaines

- Parent/Child (Parent/enfant) : processus et données affectés
  - Conception basée sur un flux de processus.
  - N'oubliez pas que les domaines parent peuvent accéder à toutes les données des domaines enfant.
- Domaine « Contains » : seules les données sont affectées. Par exemple, l'ajout d'un SP dans le TOP Contains du diagramme n'entraîne pas l'exécution des processus du SP dans le domaine TOP et dans les domaines vers le bas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - Accorde des droits d'accès aux données aux personnes de groupes qui ont besoin d'un accès dédié à certains domaines.
  - Contient des causes ou des conditions à ajouter aux requêtes de base de données qui peuvent entraîner des problèmes de performance avec des ensembles de données et de domaines volumineux.
- Visibility (Visibilité) : hiérarchie qui est toujours visible par les utilisateurs une fois que vous fournissez l'accès. Seules les données sont affectées, et non les processus.
  - Accorde l'accès aux données d'un domaine à un autre domaine qui n'avait pas cet accès lors de la création de la hiérarchie parent-enfant.
  - Permet aux utilisateurs de voir toutes les données dans les domaines pour lesquels ils ont une visibilité d'accès, tout le temps, quel que soit l'enregistrement sur lequel ils travaillent.

Remarque :
Utilisez cette option avec parcimonie, car la visibilité peut entraîner un accès complet que vous n'avez peut-être pas l'intention d'accorder.

Principes de base de la définition d'une hiérarchie des domaines

Cas d'utilisation avec et sans restriction pour la séparation de domaines.

De nombreux SP ont des clients qui déclarent implicitement que l'accès à leurs domaines doit être fortement réglementé, ce qui restreint l'utilisation de la fonction « contains » dans le domaine TOP. Le diagramme suivant explique comment atténuer cette réglementation en divisant les domaines en domaines avec restriction (Restricted) et sans restriction (Unrestricted).

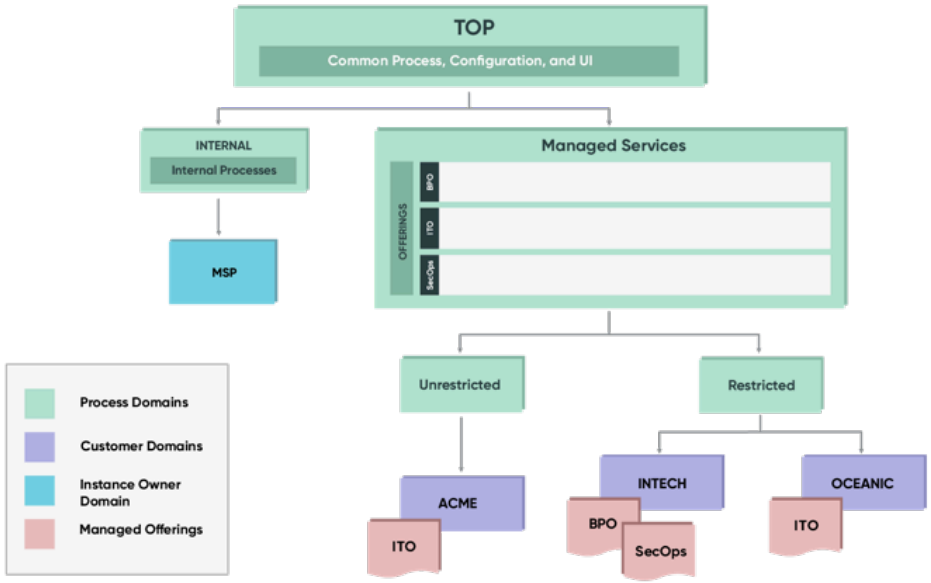
1. Les clients se trouvent dans un « vertical » spécifique de la hiérarchie de séparation de domaines Cela signifie qu'ils n'utilisent que des processus définis dans leur domaine et tous les domaines parent au-dessus du leur dans la hiérarchie. Tous les processus définis dans les domaines qui ne sont pas dans leur hiérarchie parent-enfant linéaire ne s'appliquent pas.

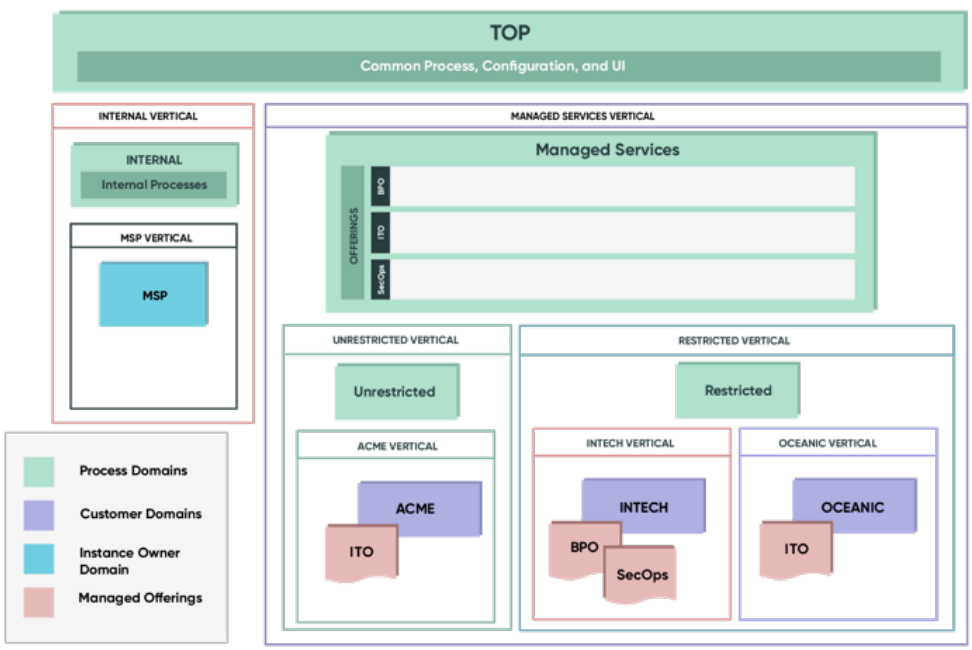
Remarque :
Les clients ou « locataires » sont des entités qui sont séparées les unes des autres, contrairement aux départements ou aux unités business, qui se partagent les ressources entre elles.

2. Les super verticaux (restreints, services de gestionnaire, etc.) sont autorisés tant que les clients n'appartiennent qu'à l'un d'eux.
3. Les services, produits ou offres qui doivent être disponibles horizontalement pour tous les clients ne sont pas définis dans des hiérarchies de domaines distinctes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Traduction automatique

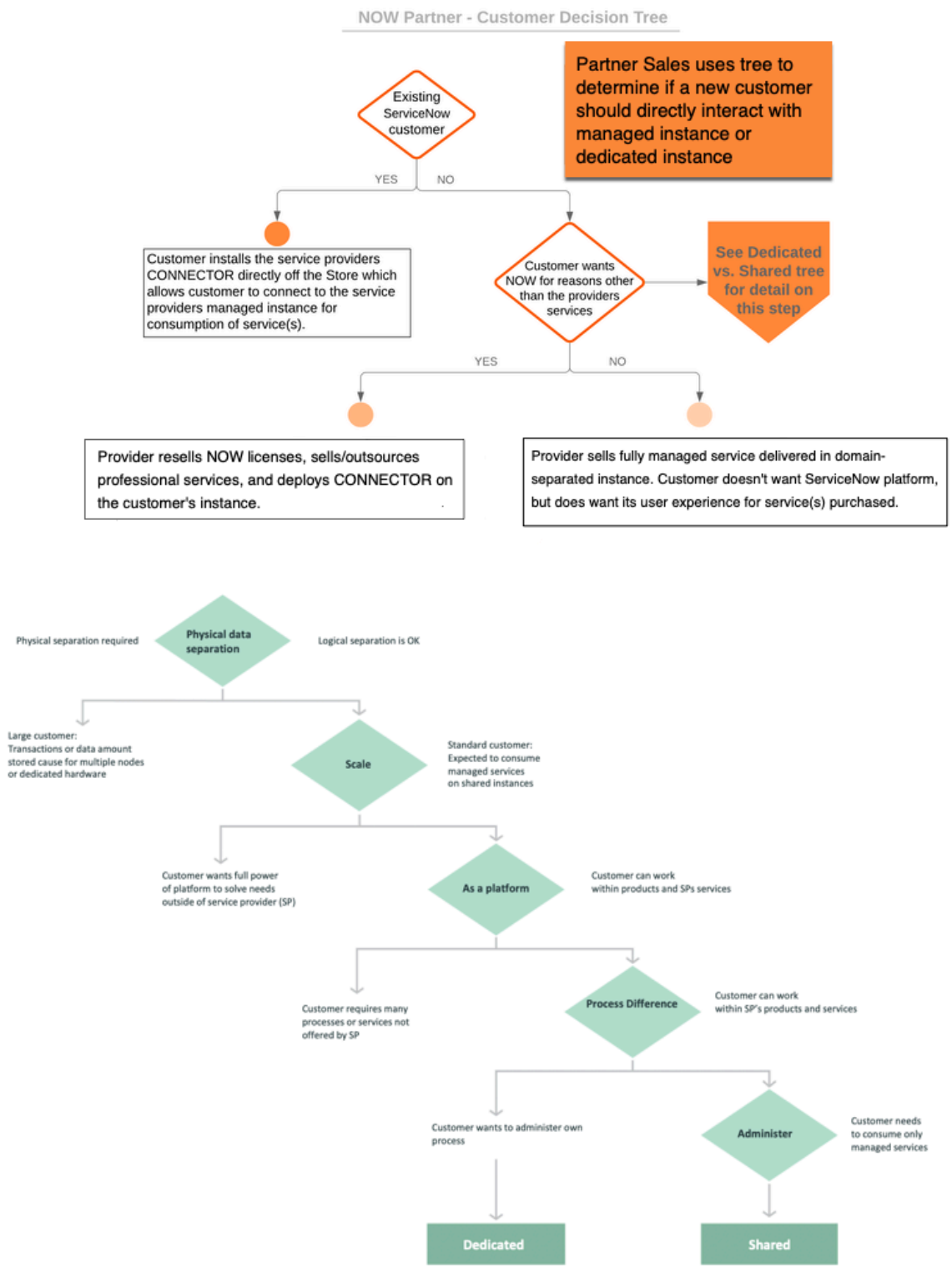
Voici quelques cas d'utilisation :

- Sous TOP, vous pouvez créer deux domaines, *Unrestricted* (Sans restriction) et *Restricted* (Avec restriction).
  - Placez les clients et leurs domaines qui n'ont pas de visibilité SP sous Unrestricted.
  - Placez les clients et leurs domaines qui ont cette exigence sous Restricted.
- Les administrateurs système peuvent alors utiliser les fonctions « contains » et « visibility » de manière efficace et ciblée.
  - Appliquez « contains » à Unrestricted pour qu'un seul « contains » puisse accorder une visibilité à la plupart des clients.
  - Appliquez la visibilité de domaine à des domaines spécifiques selon les besoins à l'aide de « groupes de visibilité de domaine ».

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Arborescences des décisions client

Le diagramme suivant montre comment choisir le modèle de hiérarchie qui vous convient. Vous pouvez choisir des hiérarchies distinctes, hybrides ou partagées, en fonction des processus et des fonctionnalités souhaités dans vos structures de domaine.



Pour en savoir plus sur l'architecture des hiérarchies, consultez Architecture de référence du fournisseur de services.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

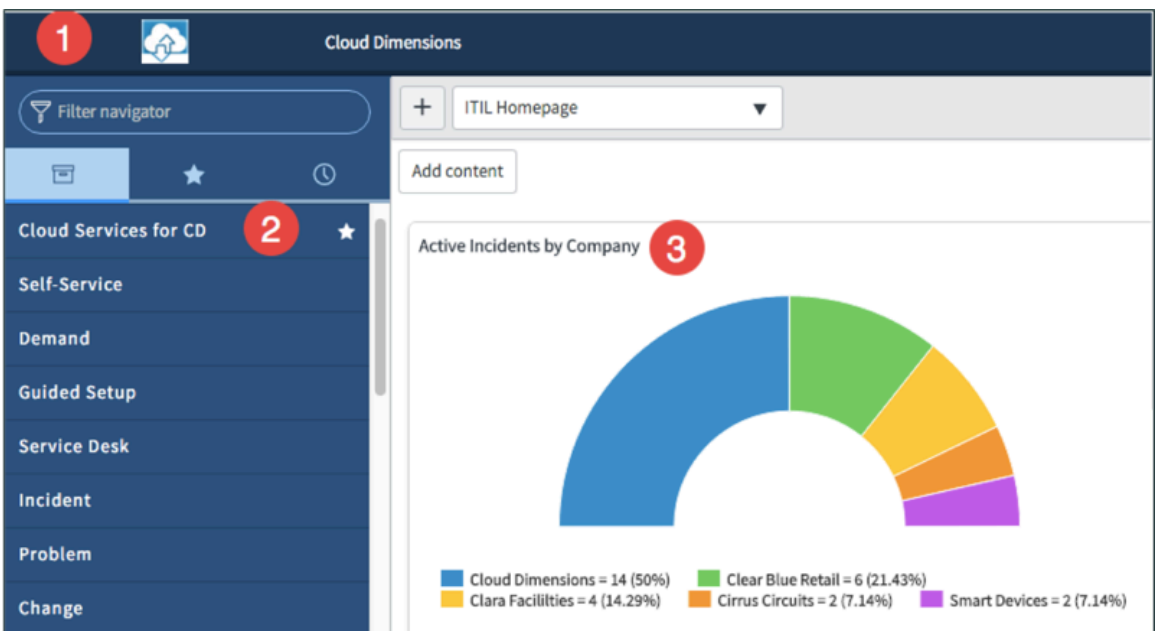
Traduction automatique

Séparation de contexte et de domaine

Le contexte de la session d'un utilisateur détermine les processus, les données et l'interface utilisateur à mesure que l'utilisateur parcourt les vues de listes, les pages d'accueil, les rapports et les articles de la base de connaissances. Le contexte est déterminé par les processus que vous créez, les règles métier que vous définissez, vos workflows et d'autres facteurs.

Contexte de la session utilisateur

De nombreux facteurs déterminent le contexte d'une session utilisateur, tels que les profils d'utilisateurs, les groupes, les critères de l'entreprise, etc. Dans le diagramme suivant, vous voyez que les incidents créés par une entreprise font partie du contexte.



Dans cet exemple, l'utilisateur possède un domaine d'accueil Cloud Dimensions.

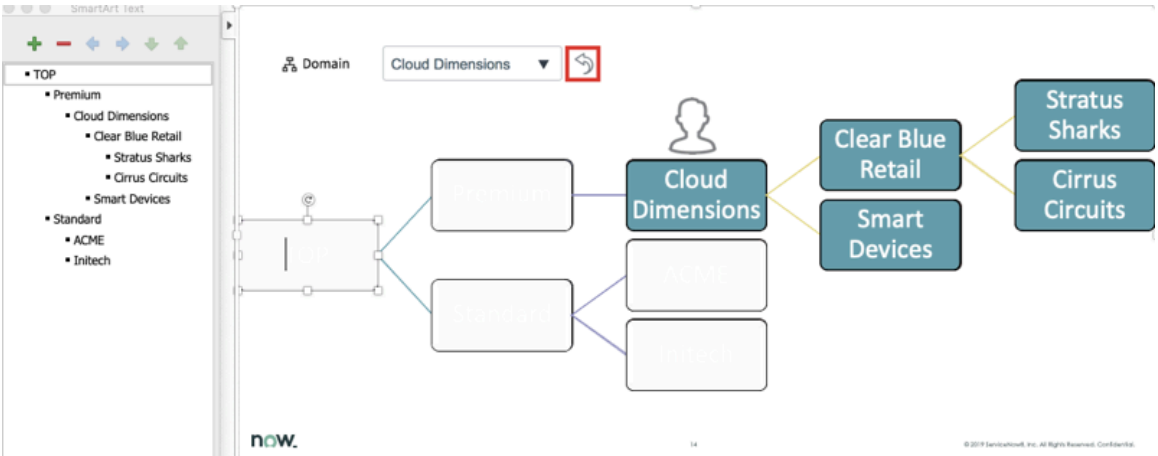
1. La marque reflète les paramètres du domaine Cloud Dimensions et de l'enregistrement de société.
2. Le navigateur d'application affiche les éléments hérités des domaines de niveau supérieur, ainsi que les modules définis dans le domaine Cloud Dimensions.
3. Les pages d'accueil et les données de liste reflètent les données visibles par l'utilisateur. Ces données sont basées sur le contexte de la session de l'utilisateur. Dans ce cas, l'utilisateur dans le domaine Cloud Dimensions peut voir les données dans Cloud Dimensions, dans les domaines enfants et dans le domaine global.

Le contexte de session utilisateur commence dans le domaine d'accueil

Dans le diagramme suivant, vous pouvez voir les éléments du contexte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'administrateur système définit les domaines d'accueil des utilisateurs sur leurs enregistrements utilisateur. En règle générale, le domaine d'accueil d'un utilisateur est défini sur le même domaine que le domaine de son entreprise. Lorsque l'utilisateur se connecte, le sélecteur de domaine se définit automatiquement sur le domaine d'accueil de l'utilisateur. Les utilisateurs peuvent revenir à leur domaine d'origine à tout moment en cliquant sur l'icône flèche du sélecteur de domaine.

La liste du sélecteur de domaine comprend des domaines dans le contexte de session de l'utilisateur. Les utilisateurs peuvent limiter davantage leur contexte de session en sélectionnant des domaines enfants avec le sélecteur.

Le contexte de la session utilisateur inclut le domaine d'accueil de l'utilisateur et tous les domaines enfants. Cet ensemble de domaines dans le contexte de la session de l'utilisateur est ajouté automatiquement à chaque requête envoyée à la base de données. De cette façon, les résultats sont limités aux données de ces domaines et aux données globales. Ce processus est intégré dans le code compilé qui n'est pas accessible.

Les comptes de services utilisés pour les intégrations disposent également d'un contexte de session utilisateur. Il existe un contexte utilisateur et un contexte d'enregistrements, chacun avec ses propres données dans son propre domaine. Ces contextes affectent les intégrations. Les requêtes de base de données (enregistrements) sont limitées de la même manière que les utilisateurs interactifs (utilisateurs), ce qui signifie qu'elles fonctionnent normalement mais sont limitées par les contraintes configurées par le développeur.

Vous pouvez découvrir d'autres façons d'ajouter des domaines au contexte de session d'un utilisateur dans Architecture de référence du fournisseur de services.

Contexte d'enregistrement

Lorsqu'un utilisateur explore des enregistrements individuels, le contexte d'enregistrement est activé. Le contexte d'enregistrement détermine les éléments d'interface utilisateur et les processus à appliquer à l'enregistrement.

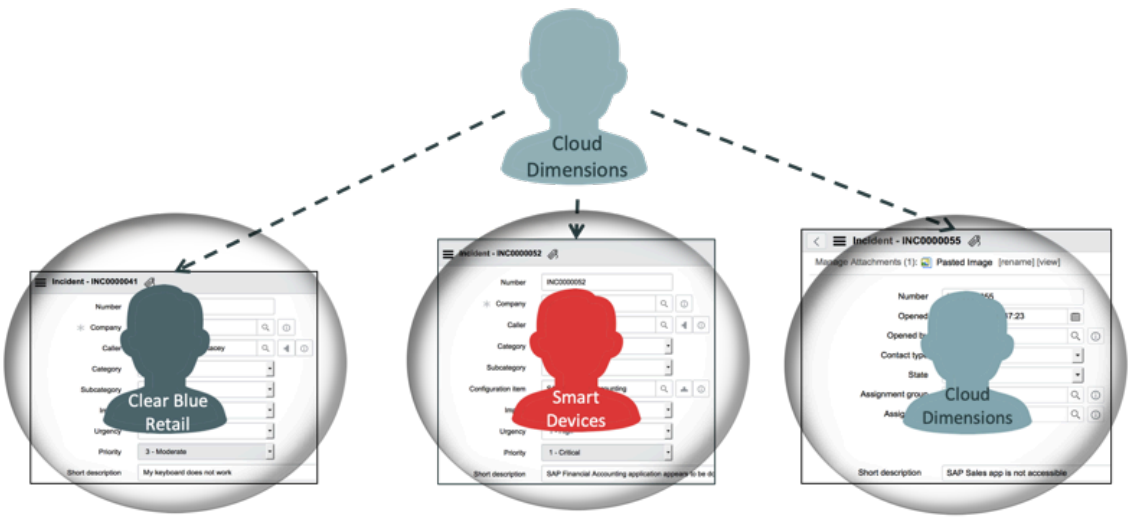
Le domaine d'un enregistrement dicte le processus, les données et la disponibilité des éléments d'interface utilisateur dans l'enregistrement.

Remarque :

- Le contexte d'enregistrement persiste même si le domaine de l'utilisateur change.
- Les utilisateurs peuvent afficher des enregistrements simultanément dans plusieurs onglets de navigateur tout en conservant leur propre contexte d'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

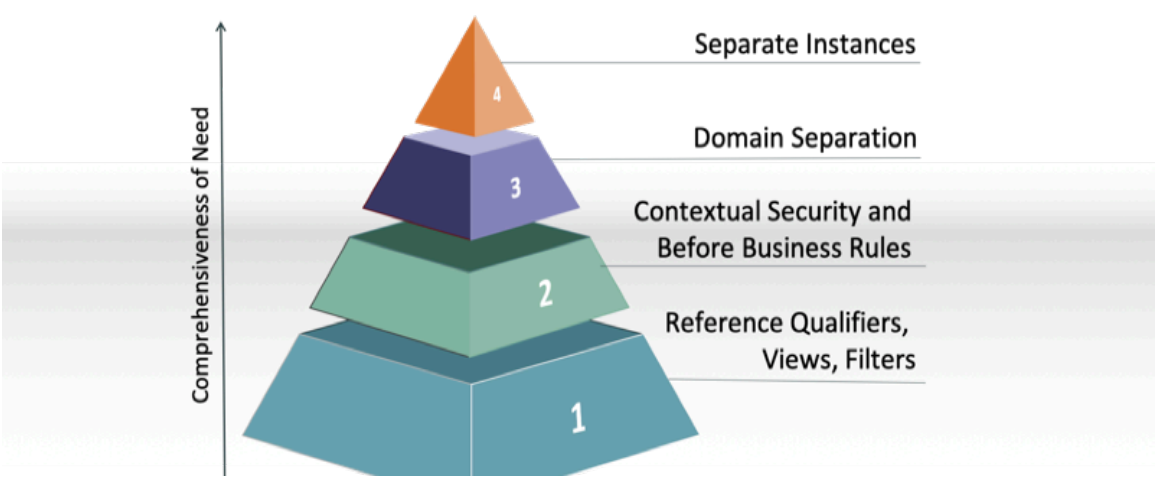


Séparer et sécuriser les données avec Domain Separation

Vous pouvez séparer et sécuriser les données sur la ServiceNow plateforme de plusieurs façons, en fonction des besoins de vos clients.

Séparer les données de plusieurs façons

Le diagramme suivant montre quatre façons de séparer les données. Vous pouvez utiliser des instances distinctes, la séparation de domaine, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence elle-même comme moyens de séparer les données.



Vous pouvez séparer les données de quatre manières :

1. Personnalisation de l'architecture de référence avec des qualificatifs et des filtres afin que les départements et les groupes d'une entreprise puissent se concentrer sur leur propre travail. En séparant les données entre ces départements ou groupes, un département ou un groupe ne peut pas voir les enregistrements d'un autre département ou groupe.
2. Ajout d'une sécurité contextuelle et de règles métier avant requête comme couches de sécurité supplémentaires pour se prémunir contre les violations de données. Consultez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Séparation de contexte et de domaine et Avant les règles métier des requêtes pour en savoir plus sur Séparation de domaine et les règles métier.

3. Ajouter un niveau de sécurité supplémentaire dans une entreprise en utilisant Séparation de domaine. Les données de chaque requête de base de données sont limitées aux données qui sont visibles dans un domaine avant l'exécution de la sécurité contextuelle et des règles métier.
4. Utilisation d'instances distinctes pour séparer les données au niveau de la base de données et de la couche application

Des instances distinctes, la séparation de domaine, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence sont des moyens de séparer les données. Ces quatre façons sont liées les unes aux autres, comme l'indique la flèche Exhaustivité des besoins dans le diagramme. La façon dont chaque couche interagit avec les autres couches dépend de la façon dont vous configurez votre configuration de séparation de domaine.

Toutes les organisations n'ont pas besoin de Domain Separation. Vous pouvez trouver d'autres alternatives, telles que des instances distinctes ou une instance unique sans domaine. Pour en savoir plus sur ces alternatives, reportez-vous à la section Évaluation de la nécessité de la séparation par domaine.

Intelligence interlocataire

Une architecture mutualisée consiste à disposer d'une seule instance desservant plusieurs locataires. Les données, les métadonnées, la logique métier et le contexte de traitement des locataires sont automatiquement gérés avec l'accès aux données supplémentaires des locataires.

Locataires uniques ou multiples

Instance à locataire unique

Vous êtes un ServiceNow client, vous avez acheté les licences et c'est à vous de décider des services que vous voulez. Vous pouvez effectuer une mise à niveau quand vous le souhaitez, afficher des aperçus de toutes les nouvelles fonctionnalités et configurer votre instance immédiatement. Être un locataire unique présente les avantages et les restrictions suivants :

- Vous avez des coûts initiaux et des frais généraux administratifs plus élevés, mais vous avez plus de liberté pour rénover et agrandir.
- L'obtention et la maintenance du personnel administratif d'instance et d'approvisionnement sont plus coûteuses. Bien que vous soyez libre de créer l'environnement selon vos besoins, vous devez vous conformer aux ServiceNow pratiques et normes recommandées.

Instance à locataires multiples

Quelqu'un d'autre est propriétaire de l'instance, peut-être un fournisseur de service avec plusieurs clients. Ils effectuent la mise à niveau quand ils le souhaitent et mettent de nouveaux services sur l'instance quand ils le souhaitent. Si vous êtes client d'un fournisseur de service, vous êtes probablement sur son instance, car vous vouliez ce qu'il offre. Plusieurs locataires ont les avantages et les restrictions suivants :

- Un personnel centralisé administre les configurations, les intégrations et les mises à niveau.
- Le propriétaire de l'instance fournit des services supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les locataires de domaine ont des coûts initiaux d'utilisation de la ServiceNow plateforme plus faibles, des coûts mensuels moins élevés car ils la partagent avec de nombreux locataires et n'ont pas besoin d'employer du personnel pour administrer l'environnement.
- Avantages partagés à partir de demandes ou de changements initiés par d'autres locataires.

Alternatives à la séparation en domaines

Vous pouvez utiliser une instance distincte comme alternative à Séparation de domaine pour vos clients. Une instance distincte vous offre la flexibilité nécessaire pour répondre aux exigences de séparation des données au sein des groupes et des départements d'une organisation avec peu ou pas d'impact sur les autres.

Instances distinctes

Avantages et inconvénients d'instances distinctes

Instance distincte	Instance unique - sans domaine
Avantages	**Avantages**
Conçu pour s'adapter à chaque client/organisation	Peut traiter des scénarios simples
Minimiser l'impact de la personnalisation sur les autres	Coût
Coordination du calendrier de mise en production	**Contre**
Séparation nette	Modifications importantes du code de base
Choisir la région CENTRE DE DONNÉES	Code du système de base modifié ignoré lors des mises à niveau
Contre	Doit également s'adresser à toutes les tables secondaires et de support
Coût	Tests approfondis requis
Alignement des instances	Aucune équipe produit pour ServiceNow faire évoluer votre code personnalisé
Effort de test pour les mises à niveau	
Duplication des efforts	
Intégrations requises	

Vous pouvez chronométrer les mises à niveau et les versions séparément pour chaque instance. Toutefois, si vous choisissez d'utiliser des instances distinctes, vous devez faire beaucoup de coordination avec d'autres personnes qui administrent des instances. En configurant une instance avec la sécurité contextuelle, les vues de formulaire, les qualificatifs de référence, les filtres et des conditions robustes, vous n'avez pas besoin d'utiliser Séparation de domaine dans votre entreprise.

Avec une instance distincte, vous pouvez traiter la séparation des données et des processus, mais vos propriétaires d'instance doivent gérer et suivre les personnalisations étendues requises pour les instances distinctes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Séparation de contexte et de domaine

Architecture de référence du fournisseur de services

Évaluation de la nécessité de la séparation par domaine

Vous constaterez peut-être que Séparation de domaine ne fonctionne pas toujours pour les organisations de vos clients. Il est préférable que vous basiez votre décision sur Domain Separation en examinant les besoins de vos clients.

Évaluation de la nécessité de la séparation par domaine

Motifs de la séparation de domaine

Ces facteurs peuvent vous aider à choisir Séparation de domaine pour les organisations de vos clients :

- Vos clients ont un alignement modéré des processus et des exigences générales de la plateforme.
- Vos clients prévoient de travailler sur des tâches en tant que prestataires plutôt qu'en tant que demandeurs.
- Vos clients ont un accord contractuel qui exige que les enregistrements de données soient isolés, mais le propriétaire de votre instance a déterminé que cette exigence peut être traitée ailleurs dans la configuration.
- Les propriétaires d'instances de votre société ont des entités entières qui fonctionnent comme des organisations physiquement distinctes et ne partagent pas de données, mais la génération de rapports complète est toujours requise. Des domaines distincts permettraient une visibilité des données lorsqu'ils sont configurés correctement.

Raisons de l'absence de séparation de domaine

Ces facteurs peuvent indiquer des raisons pour lesquelles les organisations de vos clients peuvent ne pas vouloir configurer Séparation de domaine :

- Vos clients veulent administrer leur environnement, en avoir la pleine propriété et définir la feuille de route de l'expansion.
- Vos clients exigent que les données et les processus au niveau physique ou de la base de données soient complètement isolés.

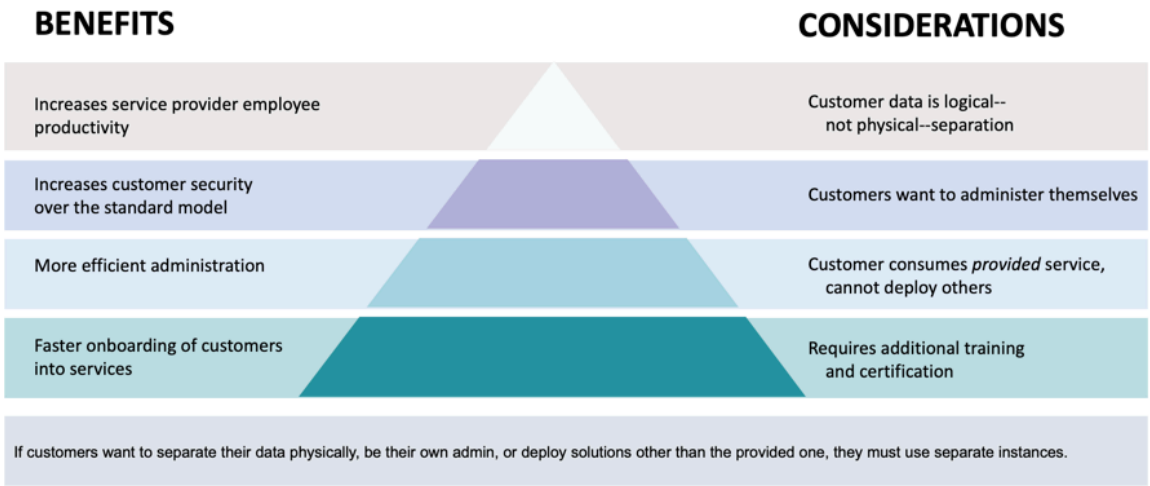
Remarque :

Les instances séparées par domaine contiennent une base de données partagée, ce qui compromet l'exigence d'isolement.

- Les départements de l'organisation de vos clients souhaitent isoler des enregistrements. (Les contrôles d'accès peuvent suffire.)
- Vos clients veulent tous leurs propres processus, règles métier et workflows.
- La culture d'entreprise est celle de la non-collaboration entre les organisations de vos clients.
- Vos clients interagissent avec la plateforme en tant qu'utilisateurs finaux uniquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

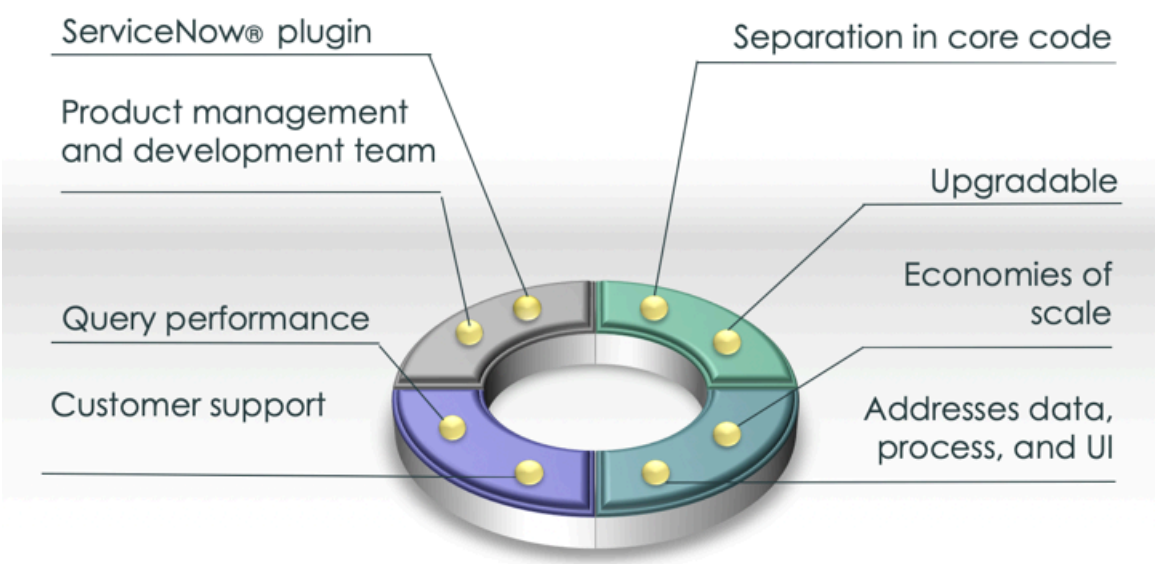


Avantages de Domain Separation

Séparation de domaine peut fonctionner mieux pour les organisations de vos clients que toute autre méthode de séparation des données entre groupes et départements.

Les avantages de Domain Separation en un coup d'œil

Vous pouvez activer Séparation de domaine avec un module d'extension ServiceNow dont la fonctionnalité est intégrée à la plateforme principale. La configuration des domaines distincts est gérée par un chef de produit qui est épaulé par une équipe de développement. Les améliorations et les correctifs relatifs à la fonctionnalité Séparation de domaine sont inclus dans ServiceNow les versions et prêts à être utilisés par les clients. Pour obtenir de l'aide sur la séparation de domaine, vos propriétaires d'instance peuvent utiliser Service client et assistance des ressources, telles que Service Portal .



Fonctionnement d'une requête de base de données avec Séparation de domaine

L'utilisation de requêtes de base de données avec séparation de domaine dans les applications de vos clients les aide à protéger leurs données. Ces requêtes accélèrent ensuite les processus de configuration et de version.

Traduction automatique

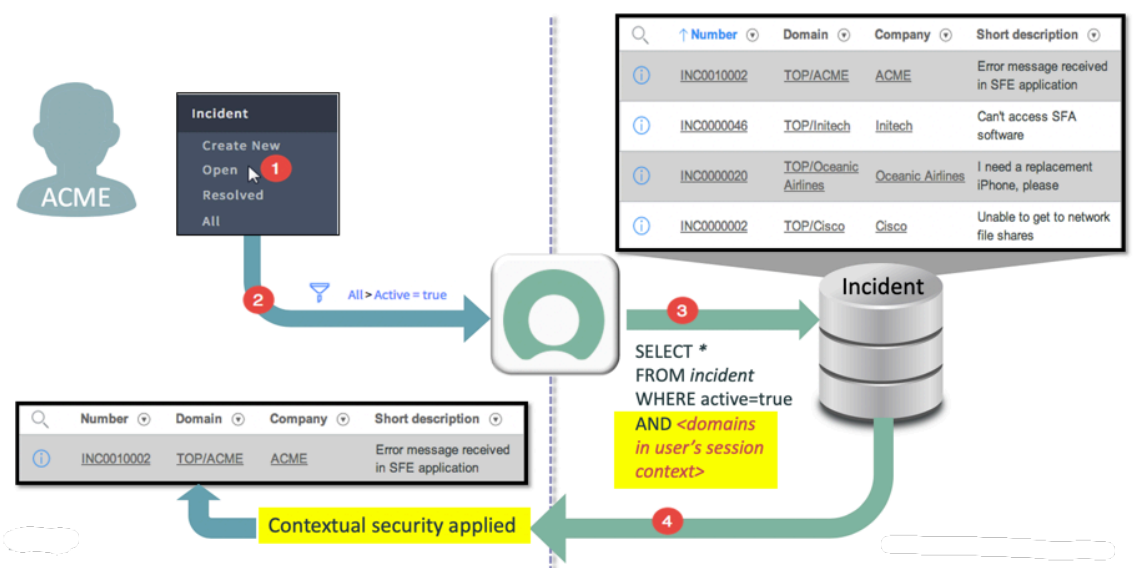
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment Séparation de domaine protège les données

Dans la figure suivante, la table Incident [incident] comporte un champ de domaine qui est hérité de la tâche de l'incident. Lorsque vous voyez ce champ de domaine, vous savez que les enregistrements de la table peuvent avoir des affectations de domaine.

Lorsque les utilisateurs se connectent, leur domaine d'accueil apparaît avec l'ensemble des domaines auxquels ils peuvent accéder. C'est ce qu'on appelle le contexte de session de l'utilisateur. Pour plus d'informations sur les contextes de session, reportez-vous à la section Séparation de contexte et de domaine.

Requête de base de données avec séparation de domaine



1. Dans un navigateur, l'utilisateur de l'une des sociétés, Acme, sélectionne le module Incidents ouverts pour afficher tous les incidents où actif = vrai.
2. Le filtre actif=vrai est soumis à l'application.
3. L'application envoie ensuite une requête à la base de données en ajoutant une clause WHERE à active=true. La clause WHERE limite les enregistrements d'incidents qui sont renvoyés aux enregistrements qui se trouvent dans le domaine de l'utilisateur ou aux domaines auxquels l'utilisateur peut accéder. Seuls les enregistrements de ces domaines sont renvoyés à l'application pour traitement.
4. La sécurité contextuelle est appliquée, limitant davantage les données renvoyées à l'utilisateur. Les enregistrements d'incidents apparaissent dans la liste des incidents ouverts.

Remarque :

Lorsque vous appliquez la sécurité contextuelle, vous créez des limites aux données qui sont renvoyées à l'utilisateur. Ces limites protègent d'autres contenus que vous ne souhaitez peut-être pas que les utilisateurs voient.

Pour en savoir plus sur la sécurité contextuelle, reportez-vous à la section Séparation de contexte et de domaine.

Remarque :

Cette logique de traitement s'applique à toutes les requêtes de la base de données, y compris celles qui sont déclenchées à l'aide d'intégrations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveaux de prise en charge de Séparation de domaine

Choisissez parmi trois catégories pour la séparation de domaine d'une application pour les organisations de vos clients.

Les applications qui prennent en charge Séparation de domaine peuvent uniquement prendre en charge la séparation des données et l'acheminement des données, disposer d'une séparation de logique métier avancée ou prendre en charge l'administration au niveau du locataire (client) de l'application. Ces définitions définissent les niveaux de prise en charge du point de vue des cas d'utilisation réels et des personnes qui les implémentent.

Niveaux de prise en charge incrémentielle ServiceNow



Niveau	Type	Résumé
Aucune prise en charge		• Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique métier pour gérer les données. • Ce niveau n'est pas considéré comme étant séparé par domaine.
Élémentaire	Gestion des données client	• Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de services de l'application. • Dans l'application, l'interface utilisateur, les clés de cache, le reporting, les déploiements, les agrégations, etc., prennent tous en compte les propriétés du domaine au moment de l'exécution. • Les propriétaires de vos instances doivent pouvoir configurer l'application pour qu'elle fonctionne normalement sur plusieurs locataires. Cas d'utilisation : lorsqu'un fournisseur de service utilise la messagerie instantanée pour répondre au message d'un client, le client doit pouvoir voir la réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau	Type	Résumé
Standard	Gestion des processus client	• Inclut le niveau de base • Logique métier : les processus peuvent être créés ou modifiés par client par le fournisseur de service. Les cas d'utilisation reflètent la façon dont l'application est utilisée par plusieurs clients fournisseurs de service dans une seule instance. • Les propriétaires de vos instances doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par client pour l'application spécifique. Cas d'utilisation : l'administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un client, mais pas pour un autre client.
Amélioré	Configuration autogérée par le client	• Inclut les niveaux basique et standard • Permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas affecter un autre client. • Les clients de l'instance doivent être en mesure de configurer eux-mêmes la logique métier et les paramètres de données MVP. Cas d'utilisation : le client d'un environnement partagé doit être en mesure d'apporter des changements en fonction de l'impact, de l'urgence ou de la priorité au sein d'un domaine.
Domaine effectif*		Dans certains cas, une fonctionnalité ou une application de plateforme peut prendre en charge les cas d'utilisation du fournisseur de service, même si le cadre de travail de domaine n'est pas utilisé. Les cas d'utilisation doivent être détaillés pour prendre en charge Séparation de domaine. Un astérisque (*) après le niveau de prise en charge indique ce type de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau	Type	Résumé
		Cas d'utilisation : avant la version New York, il n'y avait pas de prise en charge de domaine, Catalogue de services mais les propriétaires d'instances pouvaient configurer des catalogues et des éléments distincts pour chaque locataire d'une instance séparée par domaine à l'aide des critères d'utilisateur. Ainsi, chaque locataire pouvait utiliser Service Catalog à un niveau standard.

Pour afficher toutes les applications répertoriées par leur niveau de prise en charge, reportez-vous à Prise en charge des applications pour Domain Separation.

Résumé

Séparation de domaine est un cadre de travail que vous devez utiliser pour que vos applications connaissent ses clients.

Tenez compte des options du cadre de travail de domaine, des cas d'utilisation métier de vos applications, des profils et de la façon dont ils utilisent l'application avant de pouvoir utiliser le cadre de travail pour rendre votre application supportable.

Architecture de référence du fournisseur de services

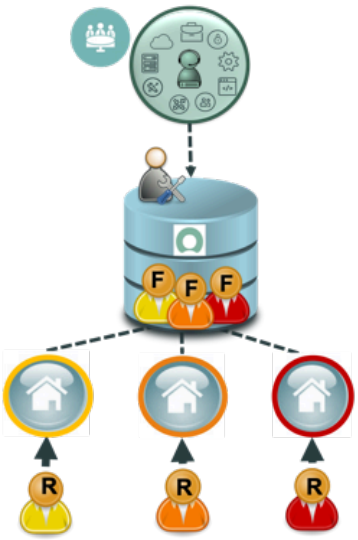
Vos clients peuvent accéder aux services du fournisseur de services (SP) à l'aide d'un portail conçu pour qu'ils puissent atteindre leur instance séparée par domaine.

Attributs de base de l'architecture de référence du fournisseur de service

- Vous n'affectez pas de prestataires à un domaine. Au lieu de cela, vous les partagez entre les domaines. Il est donc plus difficile de vérifier le nombre de prestataires que vous avez par domaine.
- Vous pouvez partager et exploiter l'administration de domaine. Cela signifie qu'il n'y a pas de surcharge et que vous pouvez optimiser les licences.
- Le nombre d'utilisateurs sur l'instance peut changer lorsque vous obtenez un nouveau client. Un nouveau client peut entraîner des dizaines, voire des centaines de milliers de nouveaux utilisateurs sur le système. Le nombre total d'utilisateurs est pratiquement illimité dans un environnement partagé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

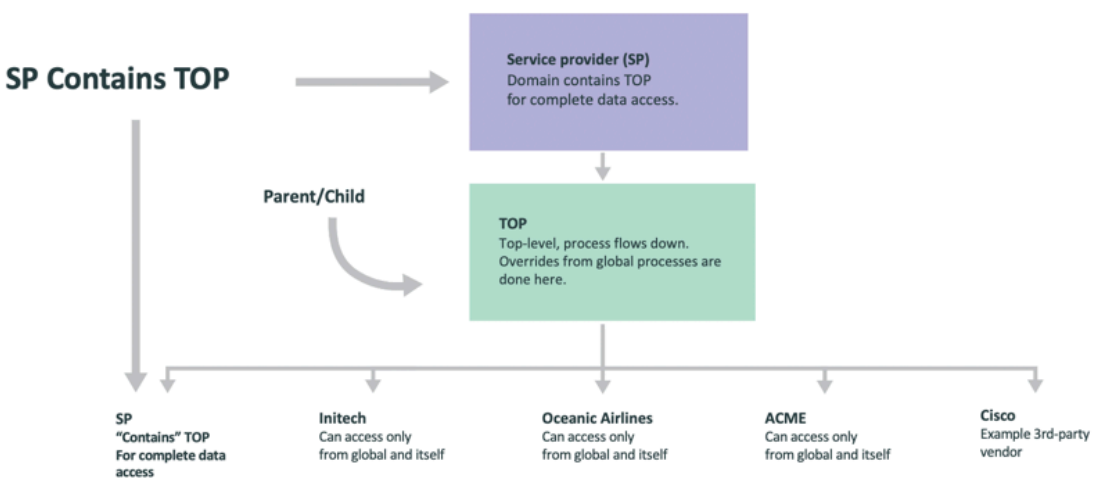
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Le portail des services SP est dédié ou partagé avec l'instance partagée SP. Les fournisseurs de services utilisent ServiceNow des instances partagées pour gérer leur prestation de services.

Hiérarchie de référence pour les instances séparées par domaine



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison de l'architecture de référence du portail de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

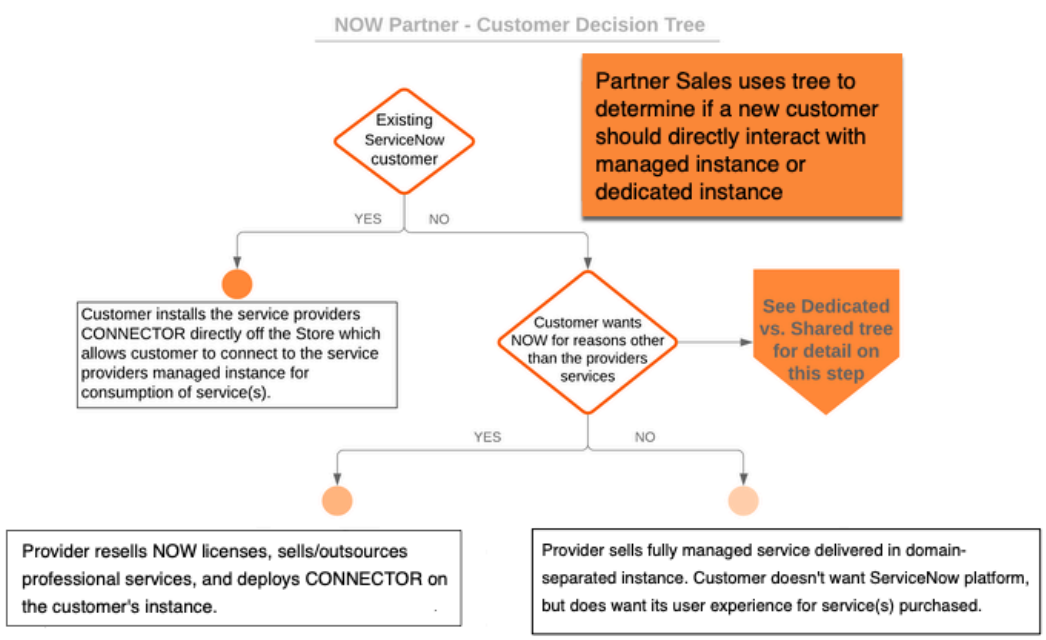
Arborescences de décision de l'architecture de référence du fournisseur de service

Vous pouvez utiliser des arborescences de décision et un tableau comparatif pour déterminer si un nouveau client doit être ajouté à une instance partagée ou à sa propre instance dédiée.

Arbres de décision

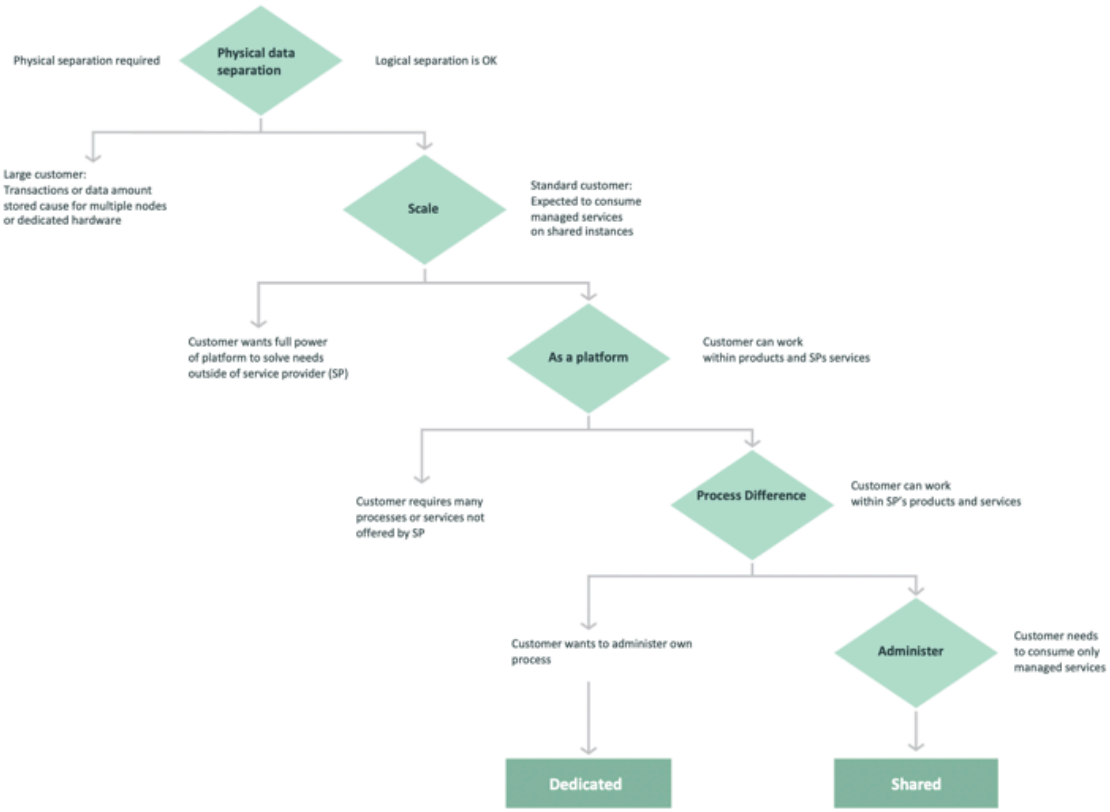
Utilisez ces arborescences de décision pour aider vos clients à décider s'ils doivent utiliser une instance gérée ou dédiée.

Arbre de décision du client



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comparaison de l'architecture de référence du portail de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

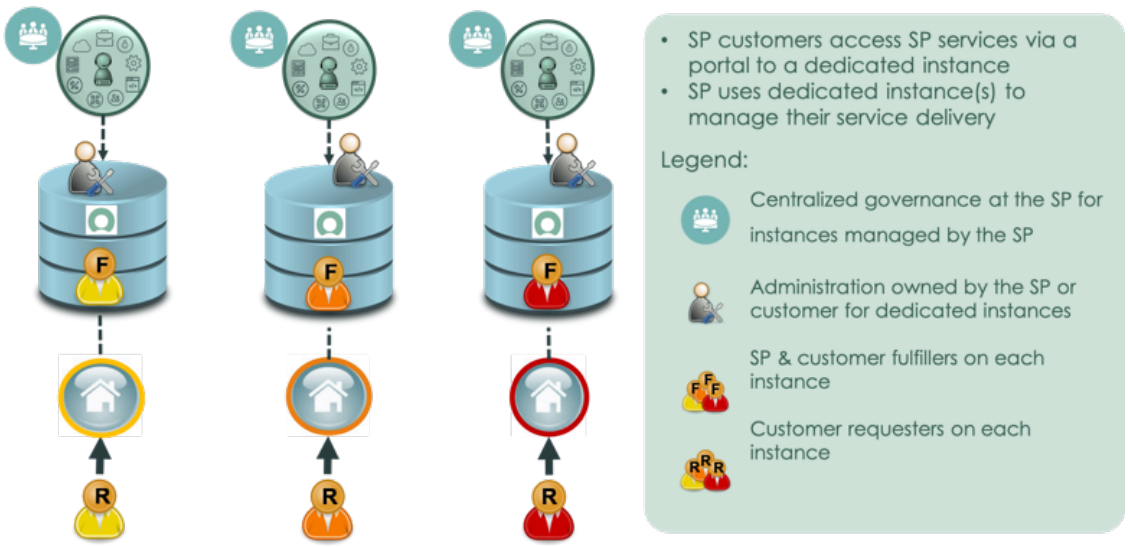
Architecture de référence du fournisseur de service pour les instances dédiées

Les clients des fournisseurs de services (SP) peuvent accéder aux services SP en utilisant un portail vers une instance dédiée. Les SP utilisent ces instances dédiées pour gérer leur prestation de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instances dédiées



Attributs

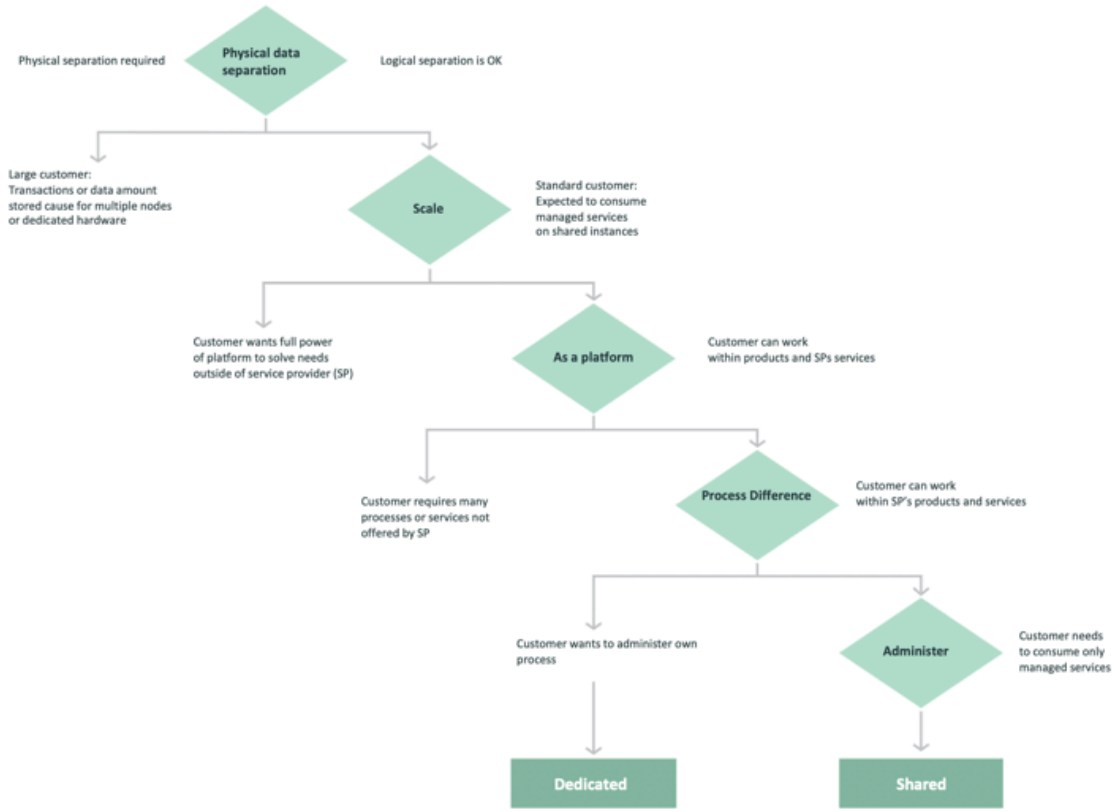
- Les instances dédiées nécessitent que vous disposiez d'une administration distincte et d'équipes dédiées. Vous avez besoin de plusieurs licences pour les administrateurs et les développeurs qui se connectent à plusieurs instances.
- Chaque instance a un nombre limité de demandeurs et de prestataires. Lorsque vous obtenez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de l'entreprise de votre client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instance partagée

Instance dédiée et instance partagée



Comparaison de l'architecture de référence du portail de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Architecture de référence du fournisseur de services pour hybride

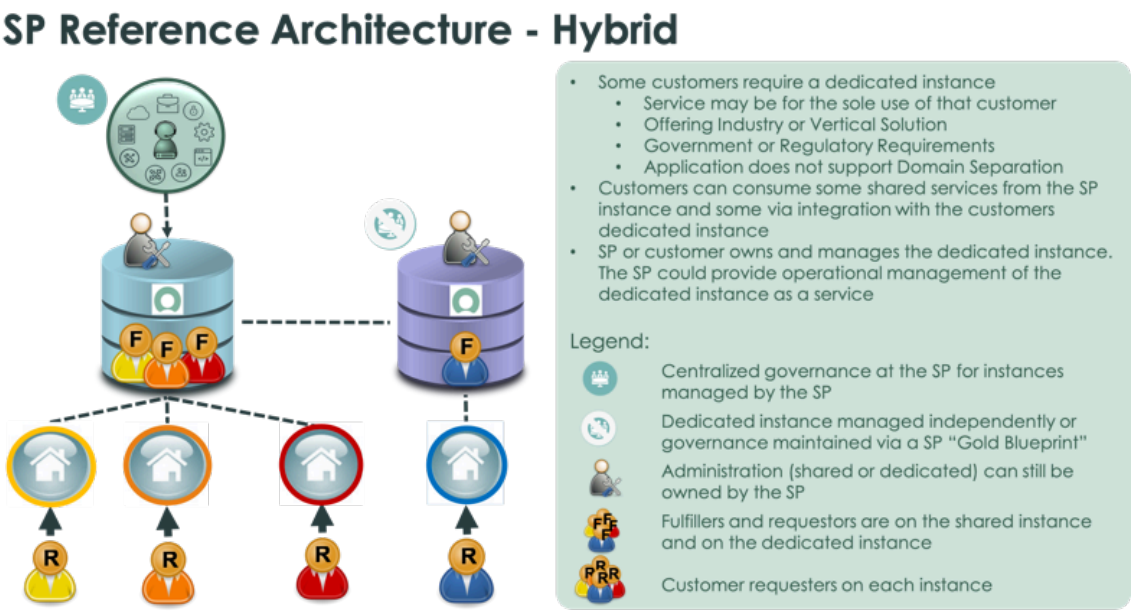
Utilisez l'architecture de référence du fournisseur de services hybride (SP) pour obtenir une solution personnalisée. Vos clients ont besoin d'une instance dédiée pour un service spécifique. Ils peuvent toujours utiliser l'instance SP partagée pour d'autres services, mais l'intégration de chaque instance est nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture hybride

Votre client peut être responsable de la livraison directe de ce service supplémentaire. Vous devez créer une solution hybride de plusieurs attributs que votre client doit fournir.



Attributs

- Vous pouvez partager et exploiter l'administration de l'instance. Cela signifie qu'il n'y a pas de frais généraux et que vous pouvez optimiser les licences.
- S'il existe une nouvelle instance pour un environnement décentralisé, l'équipe du programme est responsable et financée en conséquence en tant qu'utilisateurs administrateurs dédiés pour cette instance. Dans un environnement centralisé où toutes les instances proviennent d'un plan, vous avez besoin de licences d'administration en double.
- Vous n'affectez pas de prestataires à un domaine. Au lieu de cela, vous pouvez les partager entre domaines.
- Si un client partage à la fois un environnement partagé et un environnement dédié, il a besoin d'un prestataire dans les deux environnements. Cela signifie plus de travail pour chaque équipe, car les processus pour les instances partagées et dédiées nécessitent un travail différent pour chaque instance.
- Le nombre d'utilisateurs sur l'instance peut changer lorsque vous obtenez un nouveau client. Un nouveau client peut entraîner des dizaines, voire des centaines de milliers de nouveaux utilisateurs sur le système. Le nombre total d'utilisateurs est pratiquement illimité dans un environnement partagé.
- Chaque instance a un nombre limité de demandeurs et de prestataires. Lorsque vous obtenez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de l'entreprise de votre client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Comparaison de l'architecture de référence du portail de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

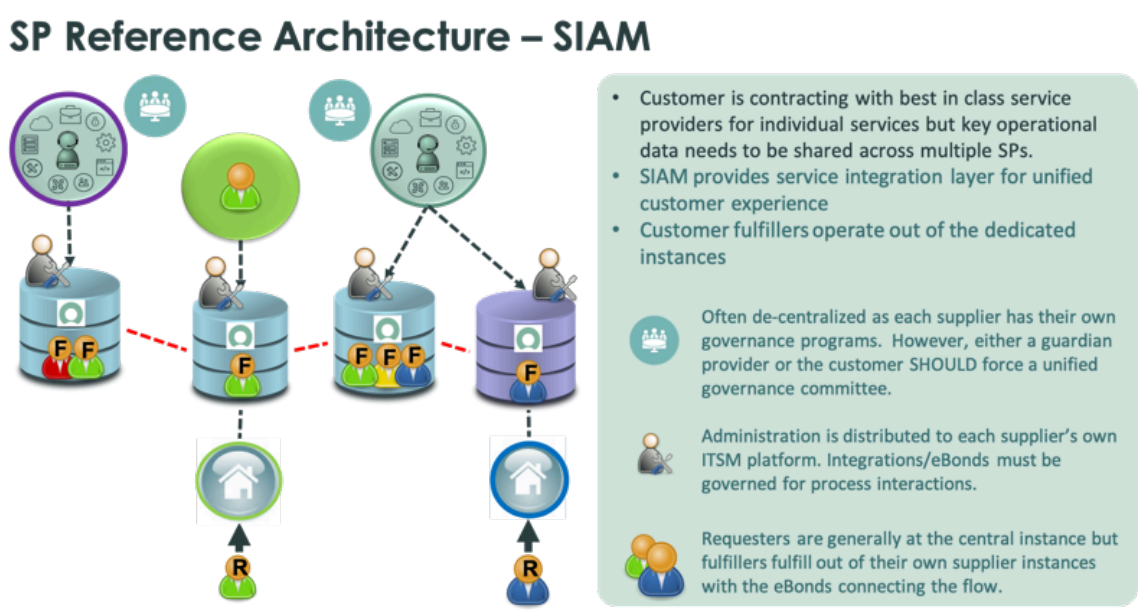
Architecture de référence du fournisseur de services pour Service Integration Management (SIAM)

L'architecture Service Integration Management SIAM (Service Integration and Management) pour fournisseur de services (SP) intègre les services pour une expérience client unifiée.

Attributs de l'architecture SIAM

- Les clients accèdent aux services SP sur un portail dédié ou partagé vers l'instance partagée SP.
- Les SP utilisent ServiceNow des instances partagées pour gérer leur prestation de services.

L'architecture SIAM en un coup d'œil



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison de l'architecture de référence du portail de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

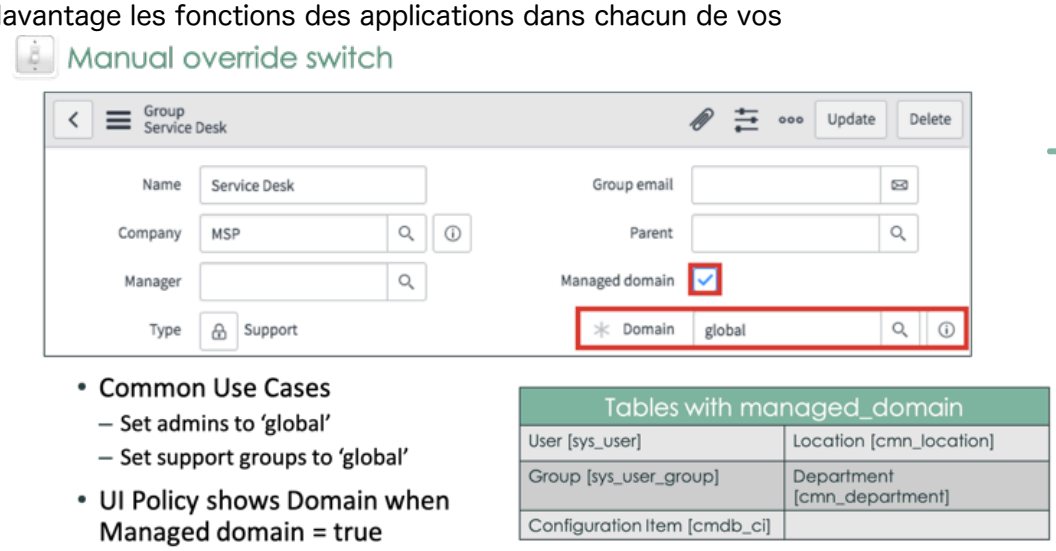
Termes de Domain Separation

Avec une ServiceNow instance, vous pouvez améliorer l'efficacité, renforcer la sécurité et augmenter les performances de vos organisations clientes. Il est utile de comprendre certains des termes les plus courants lorsque vous créez vos configurations.

Domaine géré

Dans un domaine géré, le champ **Domaine géré** permet aux administrateurs de domaine de sélectionner manuellement un domaine pour l'utilisateur, le groupe, le département, l'emplacement ou l'enregistrement de CI, plutôt que d'utiliser le domaine qui est affecté automatiquement à partir de l'enregistrement de société.

Si vous souhaitez modifier ces propriétés, vous pouvez les remplacer pour personnaliser davantage les fonctions des applications dans chacun de vos



domaines.

Tables des processus

Dans les tables de processus, si vous voyez une valeur dans le champ **Remplacements [sys_overrides],** un enregistrement de remplacement de processus existe. Cela signifie que l'administration déléguée, qui permet aux administrateurs de définir des stratégies

Traduction automatique

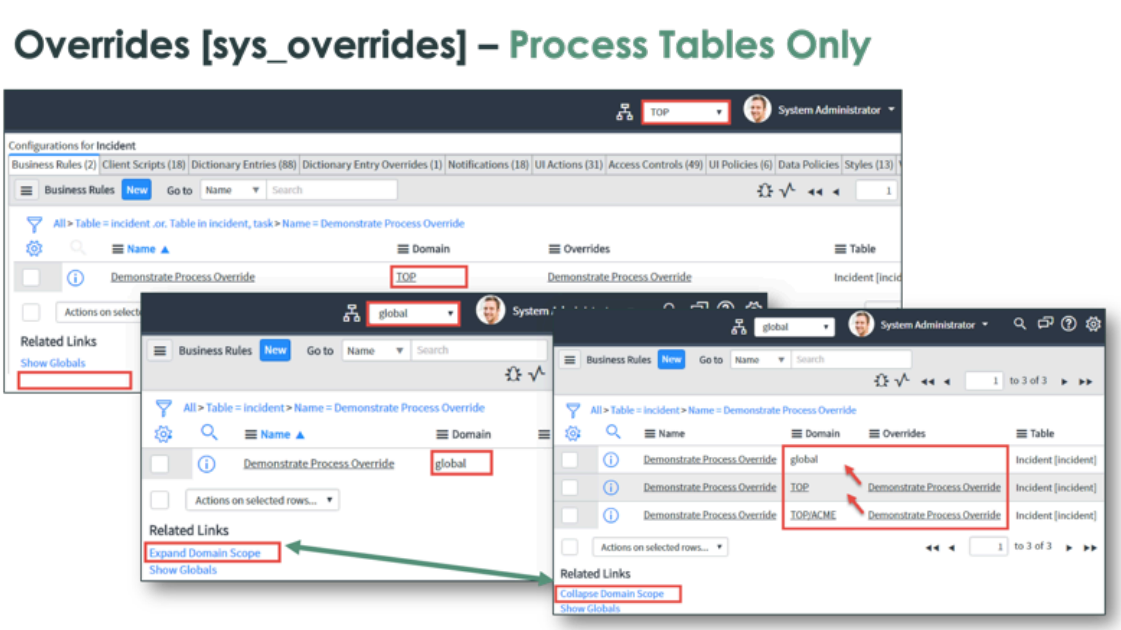
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

spécifiques à un domaine, est en vigueur. Les administrateurs dans le domaine global peuvent utiliser le lien connexe **Développer/réduire le champ d'application de domaine** pour afficher les enregistrements de remplacement.

Remarque :
Les rapports sont séparés en domaines et contiennent un champ **Remplacements** . Pour afficher tous les rapports du domaine global, utilisez le lien connexe **Élargir le champ d'application de domaine** .

Lorsque vous affichez des tables de processus à partir d'un domaine, seuls les enregistrements de processus pertinents pour le domaine sélectionné s'affichent. Lorsque vous affichez une table de processus à partir du domaine global, le lien connexe **Élargir le champ d'application de domaine** s'affiche pour vous permettre de voir tous les enregistrements de processus, y compris les remplacements. Pour afficher à nouveau uniquement les enregistrements de processus pertinents pour global, utilisez le lien connexe **Réduire le champ d'application de domaine** .

La fonctionnalité de champ d'application de domaine est utilisée uniquement pour les tables de processus et entraîne un décalage de la visibilité des données sur la table dans la direction opposée. Par exemple, un enregistrement dans le domaine parent peut être vu dans l'enfant, mais un parent ne peut pas voir un enregistrement enfant. Cela permet au processus de s'écouler vers les domaines enfants.



Types de domaines

Différents types de domaines peuvent vous aider à organiser vos processus et vos données et leur fonctionnement dans l'application ou la fonctionnalité.

Domaine client

Dans le domaine du client se trouve l'interface utilisateur, ainsi que le processus qui contrôle la façon dont les données sont utilisées.

Le domaine ACME de l'image suivante est un domaine client.

Domaine du processus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous créez des processus pour la façon dont les données sont utilisées et ce qu'elles font dans le domaine. Ces processus doivent avoir ces attributs :

- Processus et paramètres d'interface utilisateur spécifiques pour un ensemble de domaines
- Aucune donnée de base d'aucune sorte (telles que des données utilisateur spécifiques).
- Le domaine TOP de l'image suivante est un domaine de processus.

Domaine de données

Le domaine des données contient des données pertinentes pour plusieurs clients. Ces données peuvent être partagées sans partager les domaines clients réels. Chaque client a son propre domaine de données et peut y accéder.

Remarque :

Ce type de domaine n'est pas courant et peut causer des problèmes de performances s'il est surutilisé. Consultez un architecte SP avant utilisation.

Exemple : le domaine peut contenir des tâches avec lesquelles ACME, Cisco et le SP doivent tous interagir.

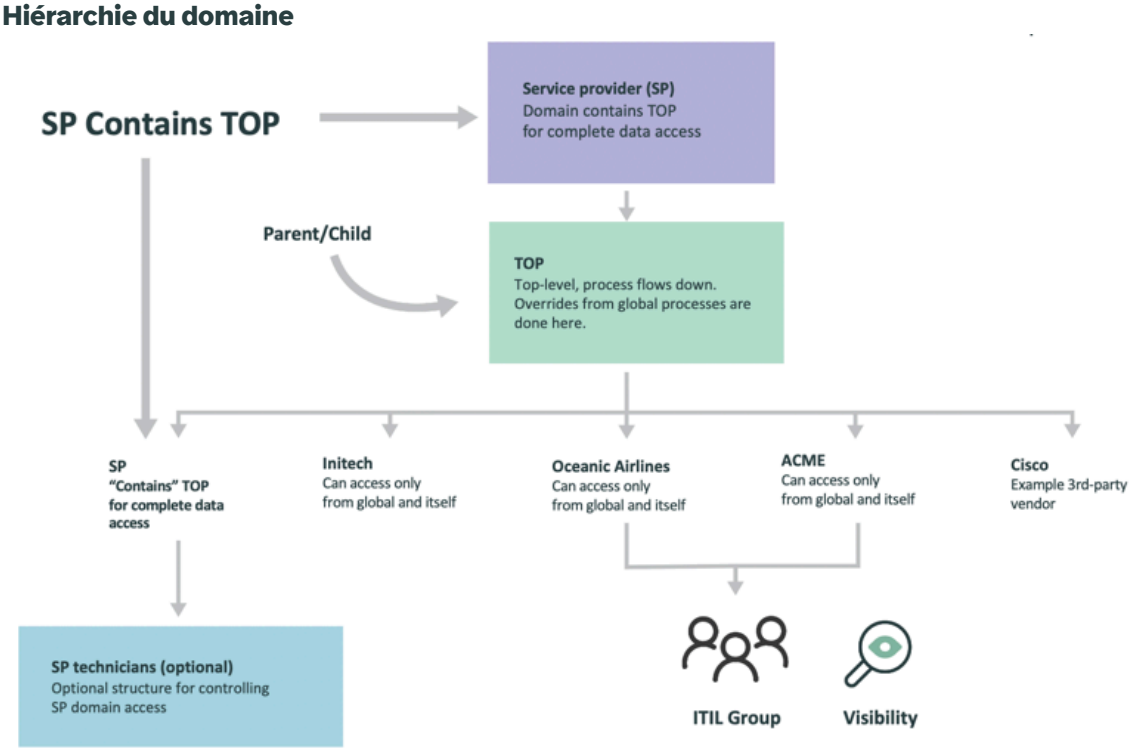
Le domaine par défaut dans l'image suivante est un domaine de données.

Données utilisateur

Les données d'enregistrement utilisateur n'appartiennent jamais au domaine global ni à l'un des domaines du processus. Les utilisateurs sont principalement créés dans des domaines clients et peuvent parfois être créés dans des domaines de données.

Les comptes administrateur sont spéciaux, car ils ne doivent pas être utilisés comme utilisateurs quotidiens de l'instance et doivent être dans le domaine global pour faciliter les fonctions administratives.

Hiérarchie du domaine



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes, admin, processus global

Listes

Dans le domaine global, si vous cliquez avec le bouton droit sur l'étiquette d'un champ de choix, sélectionnez **Configurer les choix**, puis ajoutez un nouveau choix, le choix est automatiquement transmis à toutes les listes spécifiques au domaine pour ce champ. Si la nouvelle option est marquée comme **sélectionnée**, elle est ajoutée comme active. Si la nouvelle option est marquée comme **disponible**, elle est ajoutée comme inactive.

Administration des instances

Les administrateurs du propriétaire de l'instance doivent gérer toute la création, la modification et la maintenance des processus normaux dans une instance séparée par domaine. Les gestionnaires de domaine individuels peuvent gérer certaines parties des processus pilotés par les données. Les types de gestionnaires de domaines gèrent l'administration des utilisateurs, les adhésions aux groupes de support et les emplacements, ou gèrent les applications conçues pour l'administration des locataires.

Processus/paramètres globaux

Vous pouvez créer et gérer les processus qui affectent le domaine global, ainsi que définir les paramètres. Ces propriétés sont communes à tous les utilisateurs d'une instance séparée par domaine.

Exemples : propriétés système, contournements de dictionnaire, `sys_documentation` (étiquettes de champ), modèle de données (classes, types de CI, etc.), tables et champs [sys_dictionary] (accès restreint), indexation (index de texte ainsi que base de données), ACL, sorties d'installation, actions entrantes, pages publiques et intercepteurs.

Séparation par domaine d'une table personnalisée

Vous devrez peut-être créer des tables personnalisées dans des domaines distincts. Cette rubrique couvre à la fois la procédure et le concept derrière la séparation par domaine d'une table personnalisée.

1. Créer un champ sys_domain

Remarque :
Si une table système ou une table n'a pas été séparée par domaine par le module d'extension Domain Separation, il est préférable de ne pas la séparer par domaine.

Utilisez ces points comme guide pour créer un champ sys_domain.

- Créez un nouveau type de champ *`domain_id`* .
  - Nom de colonne : sys_domain
  - Autres attributs : définis automatiquement
- La Sys_domain_path est créée automatiquement.

Le nom **de colonne sys_domain** est réservé dans le ServiceNow AI Platform, ce qui signifie que le système le reconnaît et vous applique automatiquement le type de champ et les attributs appropriés. Cette configuration automatique crée également un champ **sys_domain_path** correspondant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez le nom de la colonne sur `sys_domain` plutôt que d'utiliser l'étiquette.
- Séparation de domaine n'est pas approprié pour toutes les tables. En général, si une table fait partie de l'instance de base et que cette table n'a pas de champ **sys_domain** , vous devez le laisser ainsi.

Un champ **sys_domain** est créé automatiquement lorsque vous créez un champ de type domain_id portant le nom « sys_domain ».

2. Ajouter une règle métier pour définir le domaine

Sans règles métier

Le domaine est défini sur le domaine actuel de l'utilisateur qui crée l'enregistrement.

Avec règles métier

Le domaine est affecté à l'aide d'une logique scriptée, généralement basée sur le champ Entreprise.

En plus d'un `champ sys_domain`, les tables personnalisées ont besoin d'une règle métier similaire à **Domaine - Définir le domaine - Tâche**pour définir la valeur du champ de domaine. En outre, vous aurez besoin de **Domaine – Par défaut – Tâche**, qui déplace les enregistrements sans domaine vers le domaine par défaut si la première règle ne parvient pas à attribuer un domaine.

Sur la table des tâches, examinez les règles métier pour Domaine. Portez une attention particulière au champ Commande. La priorité d'exécution est donnée par le champ Ordre, de faible à élevée.

La première règle qui s'exécute, **Domaine – Définir le domaine – Tâche**, tente de définir le domaine de l'enregistrement en fonction du domaine de la société de l'enregistrement.

Si la première règle ne parvient pas à trouver un domaine approprié, la deuxième règle, **Domaine – Par défaut – Tâche**, s'exécute. Cette règle définit le domaine de l'enregistrement sur le domaine par défaut.

Enfin, si le domaine d'un enregistrement de tâche change, la règle métier **Domaine – Domaine en cascade – Tâche** change le domaine sur tous les enregistrements liés à la tâche, tels que les workflows, les mesures, les SLA et les pièces jointes.

3. Ajouter une règle métier en cas d'échec de l'étape 2

Si la règle métier initiale ne parvient pas à définir un domaine et que le domaine est toujours vide ou global, une deuxième règle métier s'exécute. Cette règle examine le champ `task_for` basé sur le champ appelant ou `requested_for` . Cette règle vérifie si vous pouvez définir le domaine de l'enregistrement en fonction du domaine de l'utilisateur. Dans le cas contraire, la règle métier définit le domaine sur le domaine par défaut.

Voici un exemple de script pour la règle métier :

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Domaine – domaine en cascade – tâche

Les tâches peuvent comporter de nombreuses tables connexes qui fonctionnent ensemble pour les objectifs business. Ces enregistrements connexes comprennent le workflow, le SLA, les approbations, les pièces jointes et les e-mails. Si le domaine d'une tâche change, le domaine des enregistrements connexes doit également changer afin qu'ils restent visibles par les utilisateurs dans le nouveau domaine.

Cette règle en cascade est généralement déclenchée lorsque vous effacez des enregistrements du domaine par défaut.

Les enregistrements connexes pour un domaine en cascade contenu dans le script sont affichés de la même manière que dans l'exemple :

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Personnalisation des propriétés et des thèmes de domaine

Vous pouvez personnaliser les propriétés et thèmes d'entreprise de vos clients dans les domaines que vous avez configurés. Grâce à la personnalisation, leurs instances s'intègrent à l'aspect général de leur entreprise.

Personnalisation des thèmes et logos de la société

Sur l'enregistrement de société, vous pouvez personnaliser des thèmes de conception et des logos spécifiques pour chaque société.

Personnaliser le domaine

Par défaut, lorsque le module d'extension du fournisseur de service est installé, les règles métier standard contenues dans les tables principales entraînent la définition du domaine de l'enregistrement sur le domaine de la société associée à l'enregistrement. L'entreprise peut contrôler les tables telles que Tâche, Utilisateur, Groupe, Emplacement, Département, etc.

Avec toutes ces tables, à l'exception de la table Tâche, vous pouvez remplacer le domaine dans lequel un enregistrement est créé. Cela vous donne plus d'options de personnalisation.

Gestion de la séparation de domaine pour des utilisations spécifiques

Vous pouvez configurer des domaines distincts pour les notifications par e-mail et personnaliser les propriétés du catalogue, des tables, des utilisateurs, des groupes et des vues. Cela vous permet de fournir un comportement plus spécifique dans chaque domaine, ce qui donne plus de flexibilité à vos clients.

E-mails

Vous pouvez utiliser des domaines distincts pour les notifications par e-mail et les remplacements. Lorsque vous utilisez des domaines distincts pour les notifications, vous pouvez effectuer un contournement basé uniquement sur le domaine de l'enregistrement joint et non sur l'ensemble du domaine de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catalogue de services

Service Catalog est maintenant séparé par domaine afin que vos clients puissent voir et accéder au catalogue. Les éléments sont traités comme des conditions OU lorsque plusieurs éléments sont utilisés. Les fournisseurs de services doivent gérer eux-mêmes les catégories et les éléments afin qu'ils correspondent spécifiquement à leurs propres critères.

Utilisateurs et groupes

Utilisez uniquement les comptes administrateur du domaine global, car les administrateurs ont besoin d'accéder à tous les domaines. Faites tous vos tests d'application à partir d'un domaine réel, et non dans le domaine global. Les remplacements ne sont pas traités correctement dans le domaine global. Les administrateurs doivent également disposer de comptes d'utilisateurs en production s'ils doivent utiliser l'application.

Travailler avec les champs

Il y a plusieurs points à prendre en compte lorsque vous travaillez avec les champs. Portez une attention particulière à ces champs, car ils peuvent présenter de nombreuses variantes qui affectent vos configurations.

Listes

Il existe des listes personnelles, globales et de domaines, ainsi que plusieurs vues de chacune.

Formulaires

Il existe des listes globales et de domaines, ainsi que plusieurs vues de chacun.

Une base de données

Tous les champs que vous créez existent pour tous les utilisateurs, dans une seule base de données. Tenez compte de l'impact global avant d'en créer un.

Remarque :
Les scripts ACL ne peuvent pas empêcher un champ d'être affiché dans une liste, car ils ne s'exécutent pas. Vous pouvez ajouter une ACL LECTURE pour masquer un champ aux utilisateurs si l'ACL est uniquement basée sur les rôles.

Création de tables

Lorsque vous créez une table, vous devez ajouter un `champ sys_domain` ou `sys_overrides` . Toute table contenant des données auxquelles les utilisateurs de votre instance doivent accéder a besoin du champ `sys_domain` . Les tables qui étendent ou prennent en charge les processus et qui doivent descendre vers des domaines enfants ont également besoin du champ `sys_domain` .

Configuration de Séparation de domaine avec le sélecteur de domaine

Utilisez le sélecteur de domaine à bon escient et n'oubliez pas l'approche 80/15/5 afin de ne pas trop personnaliser et d'impacter les performances de votre instance.

Vérifiez votre domaine avant d'apporter des modifications

Le sélecteur de domaine rassemble tous les domaines dans une liste parmi lesquels vous pouvez choisir.

Si votre session expire et même si vous n'êtes pas déconnecté, votre session retombe sur le domaine de votre enregistrement utilisateur. Vous perdez également tous les rôles élevés en même temps. Dans ce cas, votre sélecteur de domaine pourrait toujours afficher

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le dernier domaine que vous avez sélectionné si le cadre supérieur de la liste n'a pas été rechargé. Pour cette raison, vous devez recharger complètement votre liste si vous avez été absent de l'instance pendant un certain temps.

Configuration au niveau du domaine TOP ou du domaine global

Séparation de domaine fonctionne mieux lorsque vous fournissez des services aux clients qui sont pour la plupart standard dans leur configuration et leur définition d'utilisateurs et de groupes. Plus vous personnalisez et créez des solutions « ponctuelles », plus vous créez une marge d'erreur. Lorsque vous créez vos processus et votre logique métier, toutes les variations doivent se trouver dans des propriétés qui fonctionnent automatiquement pour chaque client. Bien que les processus puissent toujours être ajustés selon les besoins, faites preuve d'une grande prudence lorsque vous décidez quand et dans quelle mesure créer une configuration unique pour un seul client.

Vous devez utiliser une approche « 80-15-5 » dans la configuration de vos domaines pour éviter une trop grande marge de personnalisation, et donc une erreur.

- Approche recommandée pour la configuration :
  - **80 %** ou plus **Standard**
  - **15 %** ou plus **paramétrique**
  - Moins de **5 % de configuration**
- Déterminez si un changement suggéré doit être une propriété globale ou configurable.
- Ne surconstruisez pas en ajoutant de plus en plus de personnalisation qui doit être gérée. Au lieu de cela, procédez comme suit :
  - Commencez par les fonctionnalités du système de base et vérifiez les écarts éventuels avant d'apporter des changements.
  - Recherchez des solutions sans code.
  - Utilisez des scripts côté serveur, créez des API modulaires et intégrez des propriétés séparées par domaine.
  - Si vous devez utiliser un script client, utilisez uniquement ServiceNow des API. Limitez les appels « synchrones » (ceux qui vont et viennent du client au serveur, également appelés AJAX).
  - Écrivez tous les scripts de manière logique pour qu'ils restent simples et efficaces. Appliquez des examens par les pairs des modifications de code et assurez-vous que tout le monde suit les Pratiques recommandées de séparation de domaine pour les fournisseurs de services dans cette section.

Considérations sur les performances de séparation en domaines

Lorsque vous configurez Séparation de domaine dans votre application et vos services, assurez-vous de tenir compte du nombre et des propriétés des domaines que vous créez. Trop de domaines à forte densité de propriétés peuvent avoir un impact sur les performances de votre instance.

Limiter les domaines à forte teneur en propriétés

Vous pouvez créer autant de domaines que nécessaire, mais assurez-vous de ne pas créer de domaines inutiles sur l'instance. Peser trop de domaines sur l'instance avec beaucoup de propriétés peut avoir un impact sur les performances de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le nombre de domaines n'est pas ce qui a un impact sur les performances, mais plutôt ce qu'ils contiennent. Trop de propriétés peuvent ralentir le sélecteur de domaine, ce qui ralentit ensuite l'expérience utilisateur globale de vos clients. Si vous chargez le sélecteur de domaine et que vous avez déjà un grand nombre de domaines avec beaucoup de propriétés, le sélecteur de domaine doit charger tous les domaines avant de vous donner le contrôle dans la session. Ce processus peut entraîner une panne dans laquelle vous ne pouvez accéder à rien sur l'instance tant que le sélecteur de domaine n'est pas terminé. Avant de créer de nouveaux domaines, accédez à la hiérarchie des domaines sous **Administrateur de domaine** > **Carte de domaine** et assurez-vous que vous devez réellement créer un nouveau domaine ou si une hiérarchie de domaines existante peut fonctionner.

Utilisation du Interface utilisateur principale sélecteur de domaine

Le sélecteur de référence de domaine est disponible dans Interface utilisateur principale. Avec le sélecteur de référence, vous ne chargez pas tous les domaines en même temps, mais le domaine est recherché lorsque vous commencez à entrer le nom de votre domaine dans le sélecteur de domaine.

Activez le sélecteur de référence de domaine en Interface utilisateur principale procédant comme suit :

1. Dans le navigateur d'application, saisissez `sys_properties.list`.
2. Définissez la propriété *`glide.ui.domain_reference_picker.enabled`* sur true.
3. Actualisez le navigateur.

Remarque :
Ne chargez pas un grand nombre de domaines (plus de 30) via des ensembles d'intégration ou d'importation sans effectuer d'abord des tests, sinon vous risquez de mettre votre instance hors service.

Configuration des hiérarchies de domaines

Vous pouvez éviter les ralentissements et les impacts sur les performances de votre instance en connaissant le fonctionnement des hiérarchies de domaines et en les configurant correctement.

En fonction de la hiérarchie de domaine, les utilisateurs ont accès aux données de leur domaine d'accueil et de tous les domaines enfants. Le processus descend vers les domaines enfants et les données montent.

Apportez des modifications à la hiérarchie de domaine existante uniquement lorsque cela est nécessaire. Lorsque vous mettez à jour le parent d'un domaine, le système rétablit le domaine parent avec tous ses domaines enfants qui modifient la hiérarchie de domaine. Lorsque la hiérarchie de domaine est mise à jour, le système déclenche une mise à jour en cascade sur toutes les tables associées à des domaines pour les enregistrements créés dans ce domaine. Par conséquent, un grand nombre de tableaux de support doivent également être mis à jour.

Pour les mêmes raisons, même si vous devez modifier la hiérarchie des domaines, ne faites jamais de mise à jour en masse. Imaginez le nombre de requêtes que le système doit exécuter pour modifier la hiérarchie des domaines. Faites toujours une mise à jour par petits lots. Avant de commencer le prochain lot de mises à jour, assurez-vous que les enregistrements de demande de travail de domaine (DWR) sont traités. Les DWR sont des rapports qui affichent s'il y a des erreurs après que vous avez modifié la hiérarchie de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivi des enregistrements DWR

Dans la table syslog_domain, recherchez une entrée d'informations dans la colonne Message pour **l'exécution du DWR terminée.** pour confirmer que le DWR est terminé.

Vérification des journaux de domaine pour les erreurs et les avertissements

Consultez les journaux de domaine pour rechercher des erreurs ou des avertissements dans les configurations de votre chemin de domaine, de vos processus et de votre hiérarchie.

Vous pouvez trouver les journaux de domaine dans la table Journal de domaine [syslog_domain]. Lorsque la hiérarchie de domaine est mise à jour, le système déclenche une tâche planifiée pour recalculer les chemins de domaine. La table des journaux de domaine capture les résultats.

Recherchez les erreurs et les avertissements dans cette table. Après avoir examiné cette table, vous devez résoudre ces erreurs et exécuter à nouveau le validateur du chemin de domaine.

Dans cet exemple de journal, le système a détecté dix enregistrements orphelins dans la table sys_ui_list. Les erreurs de ces enregistrements doivent être corrigées pour que le chemin de domaine puisse s'exécuter correctement.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Pour en savoir plus sur les erreurs de séparation par domaine, reportez-vous à la section Résoudre les erreurs de séparation de domaine.

Importance du domaine par défaut

L'organisation de vos domaines est une partie cruciale du processus de séparation par domaine. Si vous ne définissez pas de domaine par défaut, les nouvelles tâches et les nouveaux enregistrements d'utilisateurs vont dans le domaine global. Tout le monde peut voir les enregistrements dans le domaine global, ce qui signifie que les données peuvent être vues alors qu'elles ne sont pas censées l'être.

Lorsque vous définissez le domaine par défaut, ses enregistrements ne sont visibles par aucun utilisateur autre qu'un administrateur.

Remarque :
L'accès par défaut peut être modifié en accordant aux utilisateurs une visibilité sur le domaine par défaut ou le domaine parent.

Vous devez toujours définir un domaine par défaut pour les enregistrements de domaine sur votre instance. Le domaine par défaut est celui où le système affecte automatiquement les enregistrements de tâches et d'utilisateurs qui ne sont pas déjà affectés à un domaine.

Lorsque vous créez un domaine par défaut à partir de l'écran Administration de domaine, ajoutez le nom Par défaut dans le champ **Nom** pour le différencier des autres domaines. Cochez la case **Par défaut** pour l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérez régulièrement les enregistrements que vous créez dans le domaine par défaut et déplacez-les vers les domaines appropriés. Si les enregistrements s'affichent souvent dans le domaine par défaut, vous devrez peut-être en rechercher la raison. Idéalement, vous devez vous assurer que tous les enregistrements sont créés dans leurs domaines appropriés (et non dans les domaines globaux ou par défaut).

Contient des requêtes et l'accès au domaine

Utilisez une requête « contient » uniquement dans des cas particuliers, par exemple lorsque des utilisateurs ou des groupes ont besoin de voir des données d'un domaine auquel ils n'ont pas accès, mais que vous ne souhaitez pas déplacer ces utilisateurs vers un domaine. La création d'un domaine « contient » et l'accès d'un utilisateur ou d'un groupe pour un domaine doit être une exception, uniquement en cas d'absolue nécessité.

« Contient » est une relation de domaine à domaine qui est plusieurs-à-plusieurs et n'a aucun effet sur le flux de processus. Si vous créez un grand nombre de relations « contient » de domaine ou si vous fournissez un accès étendu, vous générez des requêtes avec trop de conditions OU. Les conditions OU sont lentes et ont un impact sur les performances de votre instance. Au lieu d'utiliser trop de relations « contient », configurez votre hiérarchie de domaines comme suit :

Exemple de requête

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

Avant de déplacer des utilisateurs vers un domaine, assurez-vous qu'ils devraient vraiment avoir accès à ce domaine. Pesez les avantages et les limites. La requête ci-dessus ne concerne qu'une seule relation qui contient. Si vous avez un domaine qui contient un autre domaine, et que ce domaine est le parent d'un certain nombre d'autres domaines, vous aurez beaucoup plus de conditions OU. Soyez prudent lorsque vous créez une carte de domaine afin de ne pas impacter les performances de votre instance.

Méthode de requête des chemins de domaine

Vous pouvez créer des requêtes efficaces avec des chemins de domaine.

Utilisez des chemins de domaine au lieu de la mise en file d'attente de domaine (sys_domain) ou de la numérotation de domaine. Les requêtes qui utilisent des chemins de domaine sont beaucoup plus rapides que la mise en file d'attente ou la numérotation.

Chemins de domaine est la méthode de requête par défaut pour les instances qui ont activé Domain Separation.

Si vous souhaitez vérifier la méthode de requête sur votre instance, recherchez les propriétés système suivantes dans le tableau de bord d'administration :

- *If domain path is enabled*: dans la table Propriétés système, vous voyez glide.sys.domain.provider=domain_paths et glide.sys.domain.paths.installed=true.
- *If domain path is not enabled*: dans la table Propriétés système, vous voyez glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false

Requêtes lentes et débogage SQL

Le débogage de SQL et des requêtes lentes peut vous aider à résoudre les problèmes de lenteur dans une instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous déboguez une instance, vous pouvez activer le débogage SQL pour rechercher les requêtes lentes ou vous pouvez rechercher les requêtes lentes en consultant la table Requêtes lentes [sys_query_pattern] en accédant aux **diagnostics système > aux statistiques > requêtes lentes**. Cette table stocke toutes les requêtes lentes dans l'instance.

Lorsque vous effectuez une recherche dans la table, recherchez les requêtes qui contiennent des domain_path pour déterminer si des requêtes lentes sont dues au chemin de domaine dans votre instance.

Si vous trouvez des requêtes lentes, essayez d'analyser pourquoi elles sont lentes.

Raisons courantes de la lenteur des requêtes

- Une requête comporte trop de conditions OU (pour plus d'informations, voir Contient des requêtes et l'accès au domaine). Dans la hiérarchie des domaines, placez l'utilisateur ou un domaine à un niveau hiérarchique où contient ou la visibilité n'est pas nécessaire.
- La méthode de requête n'est pas la méthode de requête de chemin de domaine (pour plus d'informations, voir Méthode de requête des chemins de domaine) : Si vous n'utilisez pas la méthode de requête de chemin de domaine, contactez Service client et assistance.
- Une requête a besoin qu'une base de données soit indexée afin que vous puissiez voir rapidement ce qu'il y a dans la base de données. Si vous pouvez identifier la requête lente, exécutez le « plan d'explication » pour voir s'il existe des options d'indexation disponibles. Le « plan d'explication » est une fonction de SQL qui montre la requête et ce qui s'y passe.

Avant les règles métier des requêtes

Vous pouvez utiliser une règle métier Avant requête pour faciliter la prise en charge de la ségrégation des données sur une instance. ServiceNow Les applications qui prennent en charge Séparation de domaine peuvent uniquement prendre en charge la séparation des données et l'acheminement des données, disposer d'une séparation de logique métier avancée ou prendre en charge l'administration de l'application au niveau du locataire (client).

Une règle métier Avant requête est un code supplémentaire que vous utilisez pour prendre en charge la ségrégation des données dans des environnements séparés par domaine.

Avertissement :
N'utilisez pas la règle métier Avant requête à la place du module d'extension Domain Separation. Cette règle métier n'empêche pas les fuites de données de manière aussi sécurisée que le module d'extension.

Utilisation de la règle métier Avant requête pour la ségrégation des données

Vous pouvez utiliser la règle métier Avant requête avec la ségrégation des données dans les situations suivantes :

- Lorsque Séparation de domaine n'est pas prise en charge par une ServiceNow application et que vous devez accorder ou restreindre l'accès à la table ou à la ligne à un ou plusieurs clients non internes en dehors de l'organisation du fournisseur de service.

Remarque :
Avant de commencer le développement, contactez ServiceNow l'assistance clientèle au sujet de la feuille de route de l'application pour ce produit. Des améliorations de la prise en charge de domaine peuvent être planifiées pour les versions à venir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsqu'une table est séparée par domaine, mais que l'accès à ses lignes doit être accordé ou restreint en fonction de certaines conditions qui s'appliquent uniquement à un ensemble de domaines dans le système.

Remarque :
Par exemple, un client dans le domaine X a plusieurs fournisseurs prenant en charge ce domaine et ces fournisseurs ont accès uniquement aux enregistrements qui leur sont affectés.

Points à prendre en compte avant de créer des règles métier Avant requête

Vous pouvez scripter des règles métier avant requête pour empêcher l'accès aux tables parentes et enfants en fonction d'une combinaison d'informations utilisateur, d'appartenances à des groupes, de sociétés, de rôles ou de conditions de champ spécifiques à un enregistrement. Avant la requête, les règles métier sont placées dans des domaines distincts et créées pour s'appliquer globalement, à une branche spécifique d'une hiérarchie de domaines.

- Dans la mesure du possible, créez des règles métier Avant requête dans la partie la plus basse possible de la hiérarchie de domaines, afin que la règle ne s'exécute que pour les utilisateurs auxquels elle s'applique.
- Sachez qu'il existe des scénarios dans le système où les règles métier peuvent ne pas s'exécuter ou où une interaction déclenchée par l'utilisateur peut ne pas déclencher l'exécution d'une règle métier. Par exemple, une règle métier ne s'exécute pas lorsque vous avez des cartes de transformation avec l'option Exécuter les règles métier désactivée, ou si vous avez des scripts avec le workflow désactivé.
- Renseignez toujours le champ de condition pour spécifier quand la règle s'exécute. Par exemple, vous pouvez spécifier si la règle métier s'applique uniquement à certains fournisseurs d'un domaine.

Avertissement :
Lors de la conception et du codage de règles métier (en particulier les règles métier Requête), limitez les clauses OU et les recherches dans les champs non indexés. Un trop grand nombre de clauses OU et de recherches dans des champs non indexés peuvent ralentir les requêtes ou affecter les performances de votre instance.

- Utilisez les règles métier Avant requête uniquement lorsque cela est nécessaire. Un trop grand nombre de règles Avant requête peut affecter les performances de votre instance.

Avant la requête, les règles métier s'exécutent avant les listes de contrôle d'accès (ACL) et sont généralement plus performantes. Cela est particulièrement vrai lorsque vous limitez les résultats renvoyés aux utilisateurs des environnements de fournisseur de services (SP) qui ont accès à plusieurs domaines dans le système.

Remarque :
Le filtrage des données est transparent (contrairement aux ACL) pour les utilisateurs qui ne voient pas le message . Sécurité des données restreint... lors de l'interaction avec les données.

Quand ne pas utiliser Avant la requête Règles métier et ACL

Soyez prudent lorsque vous utilisez des règles métier et des ACL avant requête pour séparer les données client. En utilisant à la fois des règles métier et des ACL, vous créez des personnalisations que vous devez ensuite gérer. Les personnalisations peuvent potentiellement entraîner des problèmes de performances. Vos équipes de développement doivent créer des processus pour s'assurer qu'ils ne cassent pas le système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Séparation de domaine offre à la fois évolutivité et gouvernance avec la méthode de requête de chemin de domaine actuelle (v3), qui est un cadre de travail largement pris en charge. Les équipes de ServiceNow la plateforme et de l'application sont responsables de la maintenance du cadre, ce qui soulage le client.

Pour les entreprises ayant de nombreux clients, une utilisation excessive des requêtes Avant et des ACL peut entraîner un dysfonctionnement des requêtes de base de données.

Comment Séparation de domaine est-elle activée ?

Vous pouvez activer Séparation de domaine avec un module d'extension ServiceNow . Un chef de produit, épaulé par une équipe de développement, gère les fonctionnalités. Des améliorations et des correctifs pour la fonctionnalité Séparation de domaine sont inclus dans ServiceNow les versions. Les propriétaires d'instance peuvent consulter Service client et assistance des ressources, telles que , pour https://support.servicenow.com obtenir de l'aide sur la Portail de services séparation de domaine.

Éviter le chemin de domaine dans les scripts

Les chemins de domaine peuvent entraîner la modification ou même la rupture des valeurs de votre script, alors ne les utilisez pas dans des scripts.

Votre script ne doit pas dépendre du chemin de domaine, car si vous modifiez la hiérarchie de domaine, le chemin de domaine est recalculé et sa valeur change. Lorsque cela se produit, vos scripts sont inutiles ou peuvent générer des erreurs ou se casser. La meilleure stratégie est de ne pas écrire vos scripts en fonction des chemins de domaine.

Utilisez le champ **sys_domain** dans vos scripts plutôt que de dépendre du chemin de domaine. Si vous modifiez la hiérarchie de domaine, le chemin de domaine est recalculé et sa valeur change, ce qui peut rendre vos scripts inutiles, générer des erreurs ou se casser. Recherchez les règles métier du système de base, qui utilisent le champ **sys_domain** , afin de vous faire une idée avant de créer vos propres scripts.

La ServiceNow plateforme ne capture pas les valeurs sys_domain_path dans un ensemble de mises à jour afin d'éviter les problèmes liés aux différences dans la hiérarchie des domaines pour chaque instance. Par conséquent, vous devez valider la hiérarchie des domaines après avoir importé un ensemble de mises à jour pour vous assurer que les valeurs du chemin de domaine de vos enregistrements sont correctes.

Pour en savoir plus sur le chemin de domaine, reportez-vous aux rubriques Demander Séparation de domaine et Centre Séparation en domaines.

Affectations de domaines

La façon dont vous attribuez un domaine a une incidence sur la valeur du champ sys_domain. Les affectations contiennent des conceptions et des propriétés commerciales qui affectent le fonctionnement de l'application dans chaque domaine.

Valeur du champ sys_domain

La valeur du champ **sys_domain** contient le domaine qui est affecté à l'enregistrement par l'un des éléments suivants :

- Société à laquelle l'utilisateur appartient
- Règle métier utilisée lors de la création de l'enregistrement
- Module utilisé lors de la création de l'enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Modèle de formulaire utilisé lors de la création de l'enregistrement
- Domaine de l'enregistrement parent
- Domaine affecté à l'enregistrement utilisateur
- Domaine de l'utilisateur qui les crée

Assurez-vous que vos stratégies et conceptions d'affectation de domaine sont bien documentées et testées afin de créer des enregistrements au fur et à mesure que ces stratégies et conceptions sont insérées dans le domaine correct. De cette façon, vous pouvez voir que les propriétés de chaque domaine doivent être dupliquées ou modifiées.

Séparation de domaine et le module d'extension Gestion du service client (CSM)

Pour un résultat optimal, soyez conscient du fonctionnement des propriétés du module d'extension CSM . Lorsque le module d'extension est activé, vous pouvez voir l'état de vos enregistrements dans vos domaines.

Les propriétaires d'instance doivent contacter Service client et assistance pour activer la *csm_auto_account_domain_generation* propriété.

Remarque :
Cette propriété système de base figure dans la table des propriétés système et est disponible après l'activation des modules d'extension CSM.

Ce que fait la propriété

Chaque fois qu'un nouveau compte est créé dans l'application Customer Service, un domaine est créé et placé sous le domaine TOP. Si le champ parent du formulaire de compte est renseigné et qu'un nouvel enregistrement est inséré, ce compte est créé en tant que sous-domaine du parent.

Que se passe-t-il si cette propriété n'a pas la valeur vrai et que le domaine est activé ?

Les nouveaux enregistrements de compte dans un environnement séparé par domaine sont automatiquement placés dans le domaine par défaut.

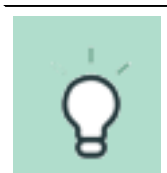
Dans la barre d'en-tête, vous pouvez voir l'état des enregistrements avec le module d'extension activé.

Aide de Domain Separation

Assistance supplémentaire avec la séparation en domaines

Vue d'ensemble vidéo de Domain Separation

Explorer, apprendre, développer



Pratiques recommandées

Trucs et astuces pour créer et développer judicieusement votre structure de domaine

Concepts pour les fournisseurs de services



Niveaux de prise en charge par application

Votre application est-elle prise en charge pour la séparation de domaine ? Voir les niveaux de prise en charge et les cas d'utilisation.

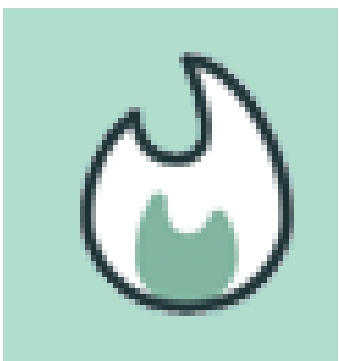
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Concepts compatibles avec la plateforme pour vous aider à résoudre des problèmes d'utilisation ServiceNow courants

Classes

- Pour les développeurs : ServiceNow Séparation de domaine du site développeur
- Pour les fournisseurs de services : Séparation de domaine pour les fournisseurs de services (connexion à l'université ServiceNow requise)



Suite Safe Workplace et séparation de domaine

ServiceNow Les applications Safe Workplace vous aident à rouvrir vos lieux de travail et à assurer la santé et la sécurité de vos employés après des situations d'urgence et des pandémies telles que la COVID-19. La suite comporte de nombreuses applications pour aider votre organisation à se mobiliser, à se rétablir et à se reconstruire.

Configuration et administration

- Mises à niveau
- Demander Séparation de domaine
- Créer un domaine
- Configuration pouvant être déléguée à des clients internes ou externes

Dépannage

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance
- Poser des questions ou y répondre dans la communauté

Configuration et administration de Domain Separation

La configuration de Séparation de domaine implique de demander l'activation d'un module d'extension, de définir des options et d'affecter des utilisateurs et des enregistrements à des domaines.

Procédez comme suit pour configurer Séparation en domaines :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Demander Séparation de domaine
2. Créer un domaine
3. Ajouter un champ de domaine à une table

Vous pouvez également effectuer ces tâches administratives de base sur les domaines :

- Activer ou désactiver un domaine
- Afficher les relations de domaine
- Élargir le champ d'application de domaine
- Créer une liste de choix spécifique au domaine

Consultez la liste Administration avancée de Domain Separation des tâches à effectuer après la configuration de Séparation de domaine et l'exécution de l'administration de base.

Demander Séparation de domaine

Toutes les fonctionnalités de prise en charge de domaine sont activées avec un module d'extension appelé **Domain Support - Domain Extensions Installer**. Les administrateurs peuvent demander l'activation de ce module d'extension.

Avant de commencer

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les `com.glide.domain.msp_extensions.installer` instances de production et de sous-production de votre organisation, en général en quelques jours à peine.

Si vous n'avez pas de chargé de clientèle, si vous décidez de retarder l'activation après l'achat ou si vous souhaitez évaluer le produit sur une instance de sous-production sans frais, suivez ces étapes.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Si le module d'extension Domain Support - Domain Extensions Installer est déjà actif, le contenu du module d'extension Domain Support - Domain Extensions Installer ne sera pas installé afin d'éviter tout conflit potentiel avec une implémentation existante.

Séparation de domaine remplace Séparation de l'entreprise. À compter de la version Helsinki, il n'est plus possible d'activer le module d'extension Séparation d'entreprise. Toutefois, si la séparation de l'entreprise est déjà active lorsque vous activez Séparation de domaine, les deux modules d'extension sont actifs simultanément. Vous pouvez contrôler l'état d'activation de la séparation de l'entreprise avec la `glide.db.separation.field` propriété.

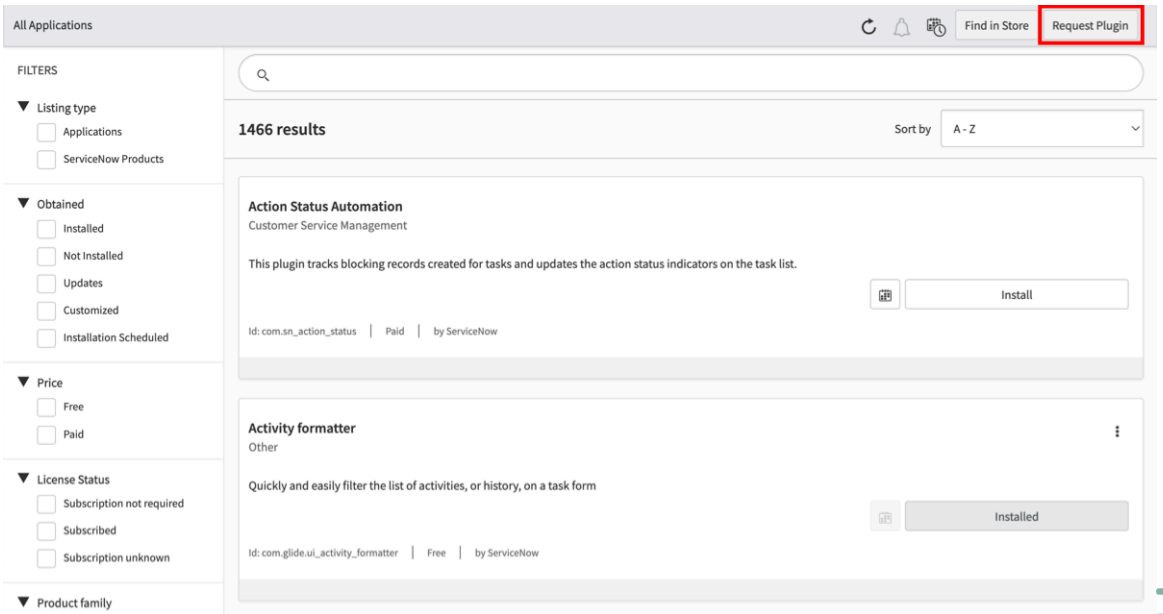
Remarque :
Les chemins de domaine sont utilisés pour tous les clients sur Helsinki et les versions ultérieures. La numérotation de domaine n'est plus utilisée. Service client et assistance peut aider à la mise à niveau.

Procédure

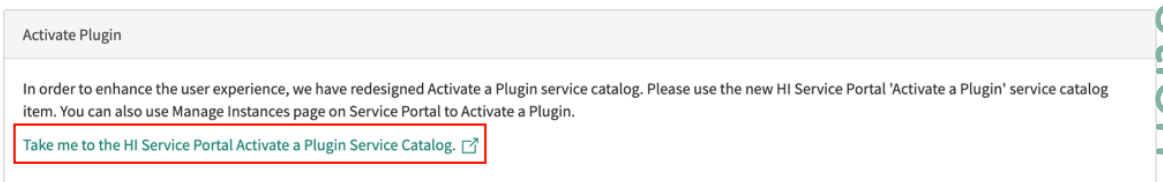
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.

Traduction automatique

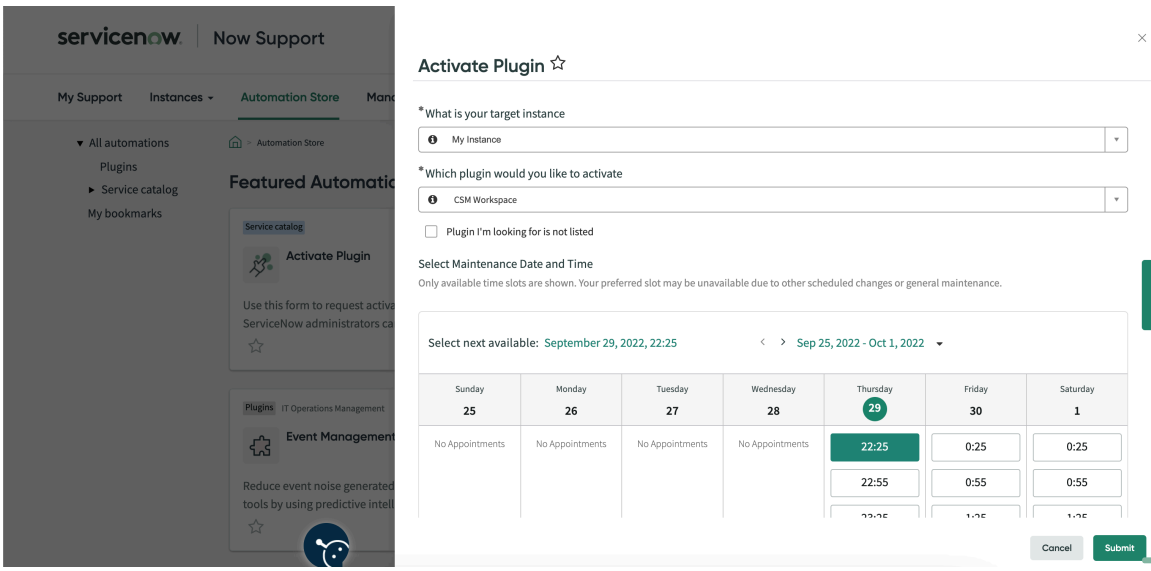
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



7. Sélectionnez **Soumettre**.
   Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Résultats

L'activation du module d'extension Domain Extension Installer active ces fonctionnalités :

- Séparation de domaine est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une politique distincte.
- Tous les enregistrements font partie du domaine global.
- Le domaine de l'utilisateur actuel détermine le domaine à utiliser lors de l'affichage ou de l'exploitation d'un enregistrement dans un domaine différent.

Information associée

Module d'extension Domain Separation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Module d'extension Domain Separation

Le module d'extension Domain Support - Domain Extensions Installer active plusieurs fonctionnalités et propriétés de séparation de domaine à la fois. Ce module d'extension est généralement appelé module d'extension Séparation en domaines.

Pratique recommandée pour l'activation du module d'extension Domain Separation

Dans le cadre du développement de Séparation de domaine, les administrateurs doivent demander l'activation de ce module d'extension. Pour de meilleurs résultats, activez le module d'extension Séparation de domaine au début du processus de développement, de préférence avant l'activation de tout autre module d'extension.

Important :
Demandez l'activation du module d'extension Programme d'installation des extensions de domaine (com.glide.domain.msp_extensions.installer) avant d'activer Séparation en domaines (module d'extension com.snc.pa.domain_support).

Si vous activez Domain Separation vers la fin de l'implémentation ServiceNow ou une fois qu'une instance a été mise en service, votre application est exposée à un risque tant au niveau des performances que du processus. Sur les instances établies, selon la façon dont les choses ont été structurées lors du développement, le risque pour la plateforme et sa facilité d'utilisation peut être élevé. Pour en savoir plus sur le processus de séparation en domaines, reportez-vous à la section Explorer la séparation de domaine.

Par exemple, lorsque le module d'extension Séparation en domaines est activé, la colonne **Domaine** (sys_domain) est ajoutée à la table de tâches et chaque enregistrement existant est automatiquement **placé dans global**. Pour utiliser un script permettant d'affecter tous les enregistrements aux domaines corrects, une hiérarchie parent/enfant établie est requise. Ces types d'actions scriptées risquent d'entraîner la corruption ou la perte de données, ainsi que d'éventuels temps d'arrêt de la production en cas de déplacement de grandes quantités de données. Une grande partie du code de la plateforme est également placée dans **des éléments globaux**, tels que les règles métier, les scripts clients, les vues de formulaire et les workflows.

Si un client crée ou modifie du code, il existe un risque pour les performances et l'ergonomie ServiceNow de la plateforme. Les propriétaires d'instances peuvent retarder considérablement leur implémentation ou subir de longs temps d'arrêt avec ce type d'approche.

Fonctionnalités du module d'extension Domain Separation

Ces fonctionnalités sont activées lorsque vous activez le module d'extension :

- Séparation de domaine est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une politique distincte.
- Tous les enregistrements font partie du domaine global.
- Le domaine de l'utilisateur actuel détermine le domaine à utiliser lors de l'affichage ou de l'exploitation d'un enregistrement dans un domaine différent.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système du domaine et préférences utilisateur

Les administrateurs ont accès aux propriétés et aux préférences utilisateur qui contrôlent le champ d'application de domaine.

Propriétés

Les nouvelles activations de Séparation de domaine restreignent automatiquement le champ d'application de domaine au domaine de l'enregistrement pour toutes les données ou tous les processus connexes. Lorsque l'utilisateur affiche un enregistrement dans un formulaire, les données connexes de l'enregistrement (telles que les données du sélecteur de référence et de la liste connexe) et les processus appliqués (tels que les règles métier et les scripts clients) sont limités au champ d'application de domaine de l'enregistrement. S'il existe des enregistrements dans plusieurs onglets, chaque onglet a son propre champ d'application de domaine en fonction de l'enregistrement ouvert dans cet onglet. Les propriétés suivantes limitent le champ d'application de domaine au domaine de l'enregistrement et au domaine de la session en cours de l'utilisateur.

Propriétés système du domaine

Propriété	Détails
glide.sys.domain.use_record_domain_for_processes	Limite le champ d'application de domaine au domaine de l'enregistrement pour tous les processus. Cette propriété ne s'applique pas aux règles métier. Les règles métier sont toujours traitées à partir de l'enregistrement de domaine. • *Type* : vrai | faux • *Valeur par défaut* : vrai • *Emplacement* : table Propriétés système [sys_properties]
glide.sys.domain.use_record_domain_for_data	Limite le champ d'application de domaine au domaine de l'enregistrement pour toutes les données. • *Type* : vrai | faux • *Valeur par défaut* : vrai dans les activations de nouveaux domaines à partir de Fuji (les mises à niveau à partir d'instances antérieures à Fuji n'ont pas cette propriété dans la table) • *Emplacement* : table Propriétés système [sys_properties]

Lorsque la `glide.sys.domain.use_record_domain_for_processes` propriété ou est `glide.sys.domain.use_record_domain_for_data` définie sur **true**, les propriétés suivantes ne sont pas utilisées, quel que soit leur paramètre :

- `glide.sys.domain.use_record_domain`
- `glide.sys.domain.use_record_domain_for_client_scripts`
- `glide.sys.domain.domain_change_notify`
- `glide.sys.domain.no_change_roles`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour obtenir la liste complète des propriétés, consultez Propriétés système disponibles .

Remarque :

Dans les nouvelles activations de Séparation de domaine à partir de la version Jakarta, le domaine de session détermine les règles métier exécutées sur la table de domaine. Dans les versions précédentes, les règles métier exécutées sur la table de domaine étaient définies en fonction de la hiérarchie du domaine nouvellement créé. Ce comportement est modifié par la `glide.sys.domain.skip_domain_insert_businessrules` propriété. Définir cette propriété sur vrai améliore considérablement les performances d'insertion de domaine.

Propriétés du champ d'application de domaine pour les règles métier exécutées sur la table de domaine

Propriété	Détails
glide.sys.domain.skip_domain_insert_businessrules	Spécifie le champ d'application de domaine des règles métier exécutées sur la table de domaine. Dans les nouvelles activations de Séparation de domaine, la valeur par défaut de la propriété est true et les règles métier sont déterminées par le domaine de session. Dans les implémentations existantes, la valeur par défaut de la propriété est false et les règles métier sont déterminées par la hiérarchie du domaine nouvellement créé. • *Type* : vrai | faux • *Valeur par défaut* : vrai dans les activations de nouveau domaine commençant par Jakarta. Faux dans les implémentations existantes.
glide.sys.domain.skip_non_global_businessrule_if_nodomain	Garantit que seuls les bus.rules du domaine global sont exécutés lors de l'utilisation de queryNoDomain() ou lorsque la table n'est pas séparée par domaine, de sorte que vous puissiez ignorer toute autre règle métier • *Type* : vrai | faux • Définir la propriété sur faux restaure l'ancien comportement et ne s'aligne pas sur ServiceNow® les pratiques recommandées. • Recommandé : séparez vos tables par domaine ; Essayez toujours d'utiliser le domaine de l'enregistrement plutôt que le domaine de la session.

Préférences utilisateur

En outre, les administrateurs d'utilisateurs peuvent définir les préférences utilisateur suivantes globalement ou par utilisateur :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférences utilisateur du champ d'application de domaine

Préférence	Catégorie	Mis à jour par	Détails
glide.domain.session_scope	Domaine	Administrateur uniquement	Si la valeur est vrai, définit le champ d'application par défaut sur le domaine de session de l'utilisateur plutôt que sur le domaine de l'enregistrement. Si la valeur est définie sur false, le champ d'application par défaut est le domaine de l'enregistrement. Les utilisateurs disposant du rôle d'utilisateur domain_expand_scope peuvent toujours modifier le champ d'application de domaine si nécessaire. • **Type** : vrai | faux • **Valeur par défaut** : faux
glide.domain.session_scope_notification	Domaine	Administrateur uniquement	Si la valeur est vrai, affiche un repère visuel indiquant que les valeurs d'enregistrement incluent un champ d'application de domaine étendu. Si la valeur est false, la notification est masquée. • **Type** : vrai | faux • **Valeur par défaut** : true

Information associée

Propriétés de l'application Domain Separation

Créer un domaine

Vous pouvez créer un domaine en créant un enregistrement dans la table [domaine].

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lors de la création d'un nouveau domaine, gardez à l'esprit les points suivants :

- Un seul domaine peut être le domaine par défaut.
- Un seul domaine peut être le domaine principal.

Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Domaines**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires (voir tableau).
4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du formulaire de domaine

Champ	Description
Nom	Saisissez un nom unique pour le domaine.
Type	Sélectionnez un type de domaine qui décrit le domaine. Par défaut, les types de domaines sont *Fournisseur*, *Client* et *MSP*. Vous pouvez également ajouter vos propres choix.
Primaire	Cochez la case si ce domaine doit être le domaine de niveau supérieur dans la hiérarchie. Le domaine de premier niveau n'a que des domaines enfants et aucun domaine parent.
Valeur par défaut	Sélectionnez si ce domaine doit être le domaine par défaut pour votre hiérarchie.
Parent	Sélectionnez le nom du domaine plus haut dans la hiérarchie qui contient ce domaine. Ce champ doit avoir une valeur pour que le domaine apparaisse sur la carte de domaine.
Actifs	Cochez la case pour rendre le domaine disponible à l'utilisation. Vous devez sélectionner cette option pour que ce domaine apparaisse dans la carte de domaine.
Description	Saisissez une description pour le domaine.

Chaque enregistrement de domaine peut également avoir plusieurs enregistrements connexes :

- Sociétés
- Contient les domaines
- Contenu par

Que faire ensuite

Pour modifier la hiérarchie de domaine, accédez à la liste connexe Domaines de contenu et sélectionnez les enregistrements de domaine qui sont les domaines enfants (contenus) de la relation de contenu.

Faire d'un domaine la valeur par défaut

A fait d'un domaine le domaine par défaut auquel le système affecte automatiquement les enregistrements de tâches et d'utilisateurs qui ne sont pas déjà affectés à un domaine.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :
Si vous ne définissez pas de domaine par défaut, les nouvelles tâches et les nouveaux enregistrements d'utilisateurs sont placés dans le domaine global.

Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Domaines**.
2. Ouvrez le domaine que vous souhaitez utiliser par défaut, par exemple Main.
3. Configurez la mise en page du formulaire pour ajouter le champ **Par défaut** .
4. Cochez la case **Par défaut**.
5. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer manuellement le domaine pour des enregistrements particuliers

Par défaut, le système affecte automatiquement un domaine en fonction de l'enregistrement de l'entreprise de l'utilisateur. Dans certains cas, cependant, les administrateurs de domaine souhaitent gérer manuellement à quel domaine appartient un enregistrement particulier.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le champ **Domaine géré** permet aux administrateurs de domaine de sélectionner manuellement un domaine pour l'utilisateur, le groupe, le département, l'emplacement ou l'enregistrement de CI, plutôt que d'utiliser le domaine affecté automatiquement à partir de l'enregistrement de société. Le champ **Domaine géré** est disponible sur ces types d'enregistrement.

- Enregistrements utilisateur
- Enregistrements de groupe
- Enregistrements de département
- Enregistrements d'emplacement
- Enregistrements de CI

Procédure

1. Accédez à l'enregistrement que vous souhaitez gérer manuellement.
2. Cochez la case **Domaine géré** .
3. Dans le champ **Domaine** , sélectionnez le domaine pour l'enregistrement.
4. Cliquez sur **Mettre à jour**.

Si vous décochez la case **Domaine géré** , le champ **Domaine** est masqué et l'enregistrement utilise la valeur de domaine de la société de l'enregistrement.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Tables séparées de domaine

Vous pouvez voir en un coup d'œil quelles tables sont séparées par domaine dans votre instance grâce à la fonctionnalité Tables séparées par domaine.

Vue d'ensemble

Utilisez la fonctionnalité Tables séparées par domaine pour voir quelles tables sont séparées par domaine. Commencez à taper « domaine » dans le filtre **Tout** pour accéder aux **tables séparées par domaine** dans le volet de navigation de gauche.

Vous pouvez filtrer cette vue pour afficher ou supprimer les noms de colonnes afin de rechercher certaines propriétés ou certains attributs inclus dans vos tables. Il existe deux types de table qui s'affichent dans la liste :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Tables avec une colonne explicite *sys_domain* présente, où le nom de **colonne** affiche *sys_domain* la valeur dans la liste.
- Tables qui utilisent l'attribut pour dériver Séparation de domaine d'un *domain_master* enregistrement référencé, où la colonne **Attributs** inclut la *domain_master=ref-field-value* valeur.

Lorsque vous utilisez les sélections Afficher la correspondance ou Filtrer dans le menu Nom de colonne, vous pouvez afficher ces deux types de tables.

Visionneuse de remplacement de domaine

Avec la visionneuse de remplacement de domaine, vous pouvez voir et gérer tous vos remplacements de processus à la fois sur l'ensemble de l'instance.

Vue d'ensemble

Plutôt que de créer une recherche élaborée de remplacements dans vos scripts, vous pouvez utiliser la visionneuse de remplacement de domaine pour les trouver rapidement. Commencez à saisir « domaine » dans le filtre **Tout** pour accéder à la **visionneuse de remplacement de domaine** dans le volet de navigation de gauche.

Le sélecteur de table de la visionneuse de remplacement de domaine affiche uniquement une liste des tables qui contiennent des remplacements d'enregistrements, ainsi qu'un décompte des remplacements dans cette table. Une fois que vous avez sélectionné une table, une liste de tous les enregistrements parents avec des remplacements est renvoyée. Vous pouvez afficher rapidement tous les **enregistrements parents**, le **domaine** de l'enregistrement parent et le **nombre** de remplacements pour chaque enregistrement.

Sélectionner **Afficher les remplacements** charge un nouvel onglet dans lequel tous les remplacements, y compris l'enregistrement parent, s'affichent dans la vue de liste standard. Sélectionnez une table dans la liste déroulante pour afficher tous les enregistrements et remplacements. Sélectionnez **Afficher les remplacements** sur un enregistrement pour afficher tous les remplacements spécifiques à un enregistrement.

Remarque :
Seules les tables avec remplacements sont répertoriées.

Pour en savoir plus, consultez Créer des remplacements de propriétés séparées par domaine .

Activer ou désactiver un domaine

Lorsque vous activez ou désactivez un domaine, l'état d'activation se répercute sur les entreprises au sein du domaine.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Lorsque vous activez un enregistrement de société, Séparation de domaine active automatiquement le domaine associé à la société. Par exemple, si vous activez la société ACME, vous activez également le domaine TOP/ACME.

Procédure

1. Accédez à l'enregistrement de domaine.
2. Désactivez ou cochez la case **Actif** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Mettre à jour**.

> **⚠ Avertissement :**
> Ne supprimez pas de domaines. Désactivez les domaines dont vous n'avez plus besoin au lieu de les supprimer.

Ajouter un champ de domaine à une table

En tant qu'administrateur, séparez une table personnalisée par domaine en y ajoutant un champ sys_domain.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

> **ⓘ Remarque :**
>
> N'ajoutez pas de domaines aux tables système de base.

Procédure

1. Accédez à la vue de liste de la table.
   Par exemple, tapez <table name>.list dans le filtre de navigation.
2. Cliquez avec le bouton droit sur l'en-tête de liste, puis sélectionnez **Configurer** > **Mise en page de la liste**.
3. Dans la section **Créer un champ** , saisissez sys_domain comme **nom** et ID de domaine comme **type**.
4. Cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.

> **ⓘ Remarque :**
>
> Tout autre moyen de créer un champ ajoute un préfixe **u_** au nom de colonne. Mais avec le champ de domaine, le système crée automatiquement le champ sans le préfixe **u_** . Vous pouvez utiliser la fonctionnalité suivante comme raccourci : Chaque fois que vous créez un champ **sys_domain**, nommez-le sys_domain et laissez le type **de** champ tel quel. Le système définit automatiquement le type de champ sur **ID de domaine** et l'étiquette de champ sur **Domaine**, ce qui vous permet d'économiser quelques clics.
>
> L'ajout de domaines aux tables système de base nécessite des tests approfondis, des mises à jour et l'ajout d'une nouvelle logique. De plus, dans de nombreux cas, le code source n'est pas accessible au client.

Afficher les relations de domaine

La carte de domaine offre aux administrateurs de domaine une représentation en lecture seule des domaines actifs sur l'instance et de la façon dont ils sont liés les uns aux autres.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Toutes les cartes de domaine doivent avoir un domaine défini comme domaine principal. De plus, chaque domaine de la carte de domaine doit répondre à ces critères :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le champ **Parent** doit être renseigné (le domaine principal est la seule exception à cette règle).
- La case **Actif** doit être cochée.

La carte de domaine ne dessine pas de relations de domaine pour les domaines qui ne répondent pas aux critères de mappage.

Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Carte de domaine**.
2. Cliquez sur les icônes plus (**+**) ou moins (**-**) sur les en-têtes de domaine pour afficher ou masquer les sous-domaines.

Sélectionner un domaine primaire

Le domaine principal indique le domaine de niveau supérieur dans la carte de domaine.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le domaine principal ne peut pas avoir de domaine parent et doit avoir au moins un domaine enfant. Il ne peut y avoir qu'un seul domaine principal à la fois. Si vous sélectionnez un autre domaine comme domaine principal, il remplace le domaine principal précédent.

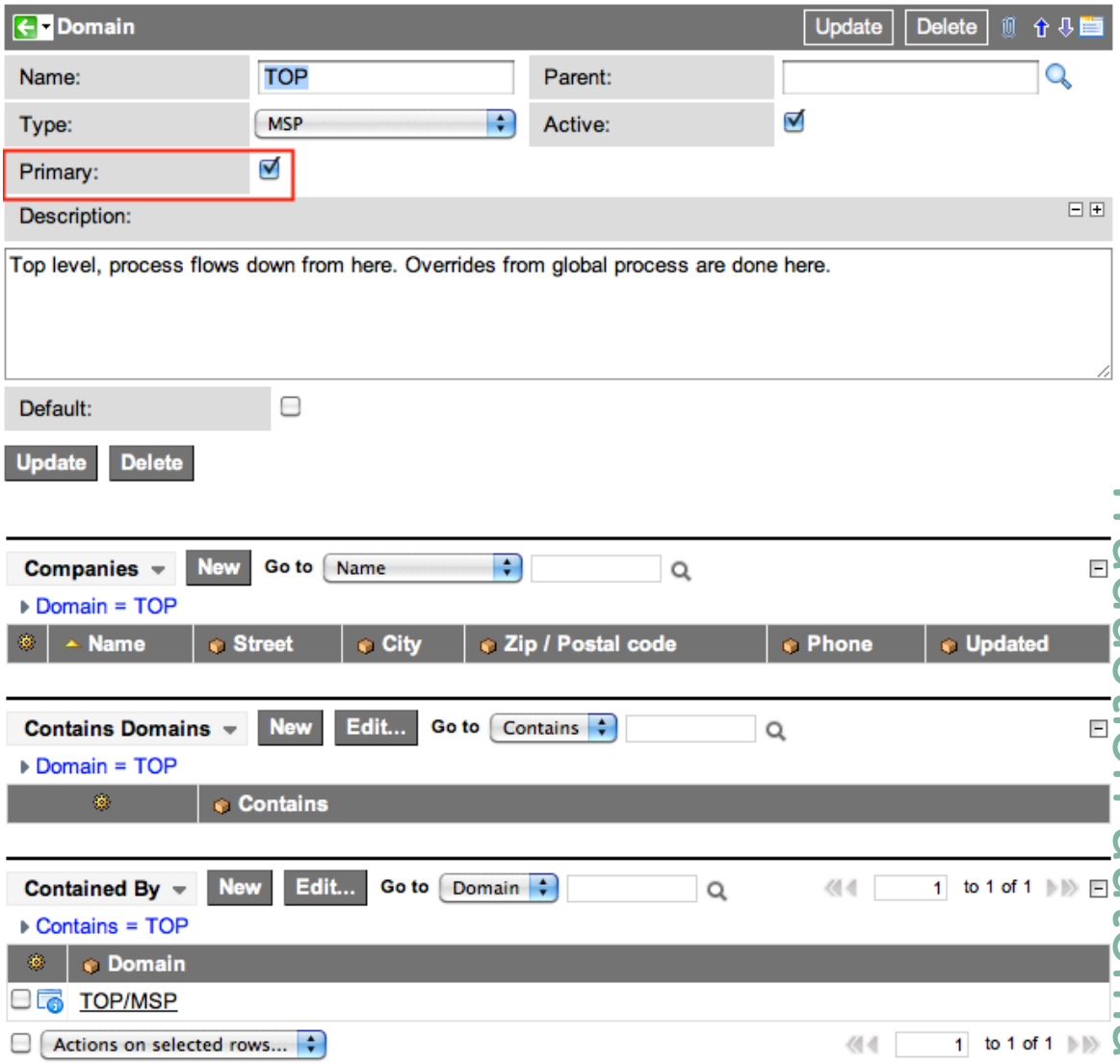
Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Domaines**.
2. Sélectionnez le domaine que vous souhaitez utiliser comme domaine principal, par exemple TOP.
3. Cochez la case **Primaire** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Mettre à jour**.



Traduction automatique

Créer Contient les relations entre les domaines

Créez une relation « contient » entre les domaines pour modifier la hiérarchie des domaines.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

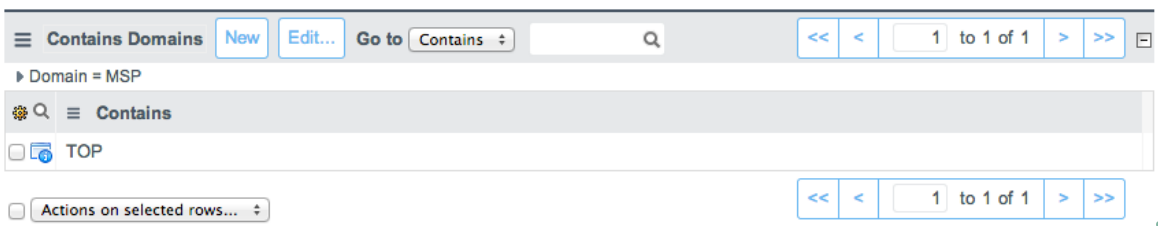
Les domaines d'une relation contient héritent des paramètres du domaine conteneur. Le domaine contenant permet aux utilisateurs de voir les données du domaine contenu ainsi que n'importe lequel de ses enfants. Les processus ne sont pas affectés par une relation contain.

Procédure

1. Accédez à la table du domaine.
2. Sélectionnez l'enregistrement de domaine qui est le domaine parent (conteneur) de la nouvelle relation contenue.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Commutez le champ d'application de domaine pour basculer entre le champ d'application de la session et celui de l'enregistrement, si nécessaire.
4. Dans la liste connexe Contient des domaines, cliquez sur **Modifier**.
5. Sélectionnez les enregistrements de domaine qui sont les domaines enfants (contenus) de la relation de contenu.
   Seuls les domaines enfants apparaissent par défaut lorsque le sélecteur de domaine est défini sur Global. Basculez le champ d'application de domaine pour voir tous les domaines.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Élargir le champ d'application de domaine

Par défaut, lorsqu'un utilisateur du domaine global affiche une table contenant une colonne **sys_overrides** , il voit uniquement les enregistrements du domaine global. Lorsqu'un administrateur du domaine global affiche une table de processus, il ne voit que les enregistrements qui se trouvent dans cette table de processus.

Avant de commencer

Rôle requis : admin

Procédure

1. Remplacez la *glide.sys.restrict_global_domain_processes* propriété par **true**.
2. Pour afficher les enregistrements de tous les domaines, cliquez sur **Élargir le champ d'application de domaine** sous Liens connexes.
3. Pour revenir à l'affichage des enregistrements du domaine global uniquement, cliquez sur **Réduire le champ d'application de domaine**.

Ajouter des domaines à une liste de domaines de visibilité

L'ajout d'un domaine de visibilité permet à un utilisateur ou à un groupe de voir et éventuellement de modifier des enregistrements d'un autre domaine, quelle que soit l'appartenance normale de l'utilisateur ou du groupe.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Il est préférable d'attribuer des domaines de visibilité à tous les membres d'un groupe plutôt que de les accorder à des utilisateurs individuels.

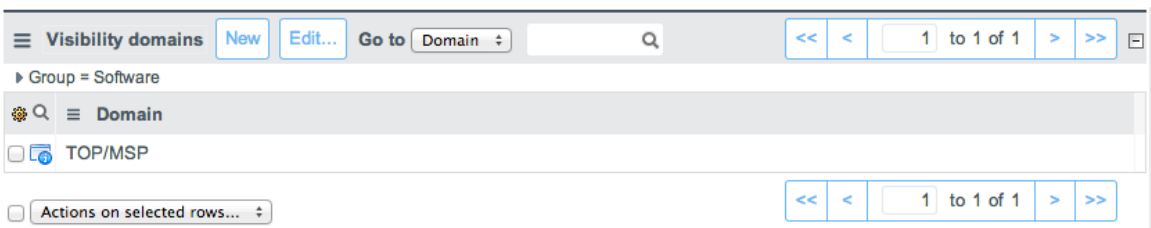
Remarque :
L'ajout d'un domaine de visibilité ne modifie pas les exigences de la règle de contrôle d'accès d'une table ou d'un enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la table des groupes.
2. Sélectionnez le groupe auquel vous souhaitez fournir des domaines de visibilité.
3. Ajoutez la liste connexe **Domaines de visibilité** au formulaire.
4. Dans la liste connexe **Domaines de visibilité** , cliquez sur **Modifier**.
5. Sélectionnez les enregistrements de domaine que vous souhaitez que le groupe ou le domaine voie.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



Accorder des domaines de visibilité à un utilisateur individuel

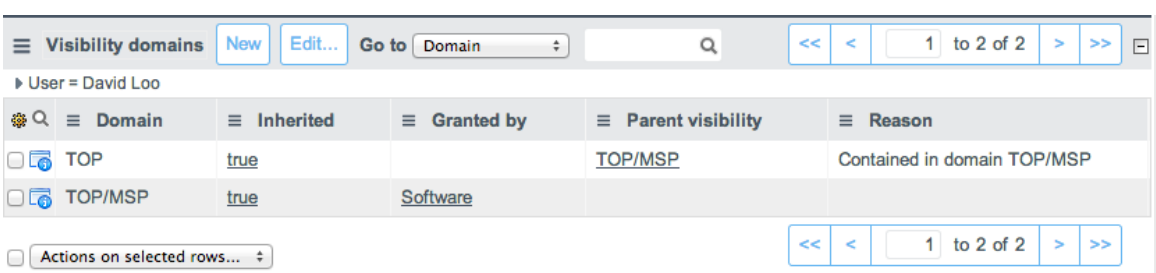
Bien qu'il soit possible d'ajouter des domaines de visibilité pour des utilisateurs spécifiques dans le formulaire Utilisateur, il est préférable de les ajouter uniquement via des groupes. Cela permet de contrôler les autorisations et l'accès en cas de changement de département ou de départ de l'entreprise.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateur**.
2. Sélectionnez l'utilisateur à qui vous souhaitez fournir des domaines de visibilité.
3. Ajoutez la liste connexe **Domaines de visibilité** au formulaire.
4. Dans la liste connexe Domaines de visibilité, cliquez sur **Modifier**.
5. Sélectionnez les domaines dont vous souhaitez que l'utilisateur voie les enregistrements.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



La liste incorporée du domaine de visibilité contient les champs suivants.

Champ	Description
Domaine	Domaine visible par le groupe ou l'utilisateur.
Hérité	Le domaine est hérité de la visibilité de domaine ou d'un domaine parent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Accordé par	Nom du groupe qui a accordé la visibilité du domaine.
Visibilité du parent	Nom du domaine parent et utilisé pour grouper les enregistrements. Si l'enregistrement parent est supprimé, tous les enregistrements ayant le même parent sont également supprimés.

Créer une liste de choix spécifique au domaine

Les administrateurs peuvent configurer des listes de choix afin qu'elles contiennent des entrées spécifiques à un domaine particulier.

Avant de commencer

Rôle requis : admin

Procédure

1. Sélectionnez le domaine dans le sélecteur de domaine où le choix doit être ajouté.
2. Cliquez avec le bouton droit sur le champ de choix que vous souhaitez personnaliser, puis sélectionnez **Configurer les choix**.
3. Mettez à jour ou ajoutez des choix.
4. Transmettre les changements par le biais du processus de changement normal, tel que les ensembles de mises à jour.

Remarque :
Les administrateurs doivent s'assurer que les choix sont uniques dans tous les domaines afin d'éviter toute confusion administrative dans le domaine global.

Si un administrateur ajoute un nouveau choix à partir du domaine global, les utilisateurs des domaines inférieurs dans la hiérarchie voient le nouveau choix à la fin de leurs listes de choix actuelles. Si le nouveau choix n'est pas actif au niveau global, il est disponible pour les utilisateurs du domaine via **Configurer les choix** , mais ne s'affiche pas comme choix actif.

Administration avancée de Domain Separation

Les administrateurs peuvent afficher des informations sur la séparation de domaine, identifier les problèmes potentiels et modifier les paramètres de configuration.

Vous pouvez effectuer ces tâches administratives avancées sur les domaines :

- Utiliser les menus de sélection de domaine
- Afficher les relations de domaine

Utiliser les menus de sélection de domaine

L'instance propose une sélection de domaine via deux formats de menu.

- Sélecteur de domaine : fournit une liste déroulante simple des domaines disponibles.
- Sélecteur de référence de domaine : active un champ de référence qui offre un filtrage et une fonction de saisie semi-automatique et de saisie semi-automatique. Utilisez ce format pour les listes plus longues.

L'emplacement de ces sélecteurs et la procédure pour les afficher ou les masquer diffèrent selon la version de l'interface utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les menus de sélection de domaine dans Interface utilisateur principale

L'affichage du sélecteur de domaine dans Interface utilisateur principale active le sélecteur de domaine par défaut. Après avoir activé le sélecteur de domaine, vous pouvez ajouter une propriété système pour activer le sélecteur de référence de domaine.

Avant de commencer

Remarque :
Séparation de domaine (module d'extension com.snc.pa.domain_support) est requis pour activer le sélecteur de référence de domaine.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur l'icône en forme d'engrenage située dans l'en-tête.
2. Dans l'onglet Général, cliquez sur le commutateur **Afficher le sélecteur de domaine dans l'en-tête** .
   Le sélecteur de domaine apparaît dans l'en-tête Interface utilisateur principale .
3. **Facultatif :** Activez le sélecteur de référence de domaine.

   Remarque :
   L'activation du sélecteur de référence de domaine supprime l'option globale de la liste. Pour revenir à votre domaine d'origine, cliquez sur la flèche de retour à côté du champ de référence. Les utilisateurs administrateurs peuvent cliquer sur la flèche de retour pour revenir au domaine global.

   a. Saisissez `sys_properties.list` dans Application Navigator.
   b. Si ce n'est pas déjà fait, ajoutez la propriété `glide.ui.domain_reference_picker.enabled` et définissez la valeur sur **vrai**.
   c. Actualisez le navigateur.
   Le sélecteur de référence de domaine apparaît dans l'en-tête Interface utilisateur principale .

Restreindre l'accès au sélecteur de domaine

Utilisez une propriété système pour restreindre l'accès au sélecteur de domaine dans Interface utilisateur principale et Next Experience.

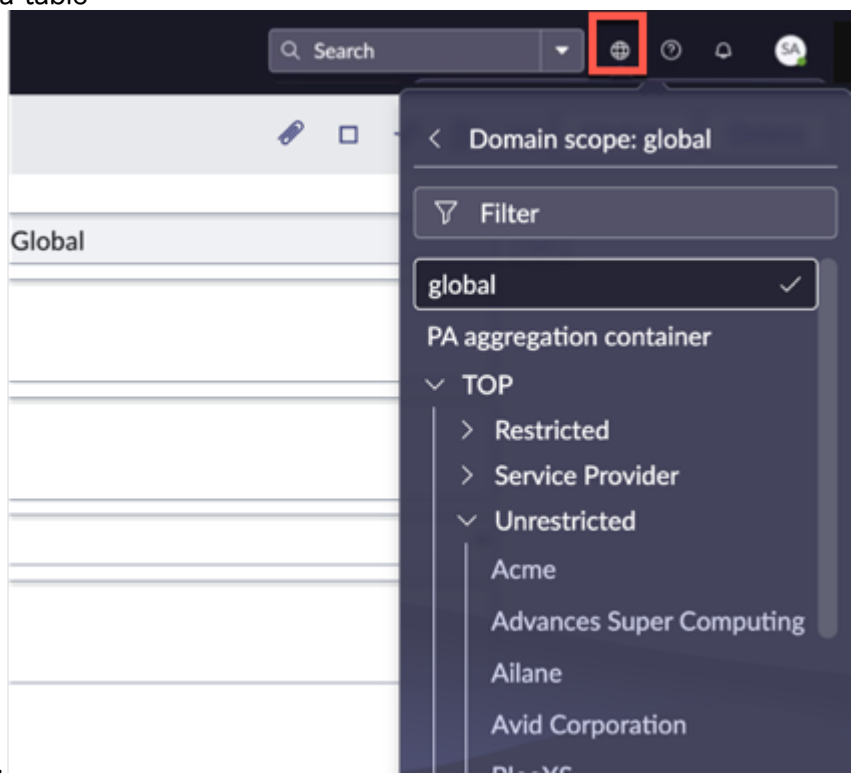
Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Par défaut, les utilisateurs disposant du rôle ITIL et des rôles qui incluent le rôle ITIL (tels que l'administrateur) peuvent accéder au sélecteur de domaine dans Next Experience. Vous pouvez accorder l'accès à d'autres rôles en les ajoutant à la propriété ou restreindre les rôles en les supprimant. Il est recommandé de limiter le rôle aux administrateurs uniquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les administrateurs peuvent accorder l'accès aux utilisateurs en créant une propriété système dans la table sys_properties.



Procédure

1. Ouvrez la table Propriétés système [sys_properties].
2. Ajoutez cette propriété : `glide.ui.polaris.domain_picker.role`
3. Configurez la valeur de la propriété sous la forme d'une liste de rôles séparés par des virgules : **administrateur, itil**.
   Pour en savoir plus, consultez Configurer les sélecteurs Next Experience

Propriétés de l'application Domain Separation

Le module d'extension Séparation en domaines dispose de deux nouvelles tables pour donner aux fournisseurs de services plus de flexibilité dans la personnalisation de leurs applications qui utilisent Séparation en domaines. Il s'agit de la table Propriétés de l'application système [sys_application_property] et de la table Valeur de propriété de l'application système [sys_application_property_value].

De nouvelles tables offrent plus d'options

Avec les applications de fournisseur de services (SP), certaines actions peuvent varier en fonction du domaine. Toutefois, la ServiceNow® table Propriétés système du système de base [sys_properties] n'est pas séparée par domaine, elle ne répond donc pas aux exigences des applications qui utilisent Séparation de domaine.

Chaque client SP peut souhaiter personnaliser ses applications différemment. Auparavant, les fonctionnalités qui pouvaient être personnalisées étaient définies comme une seule valeur globale. Les développeurs d'applications ont besoin d'une table plus flexible. Vous pouvez désormais modifier votre application sans avoir à créer de code chaque fois que vous souhaitez ajouter ou modifier la fonctionnalité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement des remplacements dans les nouvelles tables

Les développeurs utilisent généralement la ServiceNow table Propriété système [sys_properties] pour créer diverses fonctions dans les applications. Si vous souhaitez développer une application pour qu'elle se comporte différemment dans différents domaines, vous devez la personnaliser vous-même.

Dans la version Paris, la nouvelle table Propriétés de l'application [sys_application_property] simplifie cette personnalisation. Au lieu d'accéder directement à la table Propriétés système pour une valeur, la table Propriétés de l'application va d'abord à la table Application système. Cette nouvelle table stocke désormais la logique dont vous avez besoin pour configurer votre application. S'il trouve une propriété dans la nouvelle table, il utilise ce contenu. Si cette table ne contient aucune information, elle passe à la table des propriétés système de base.

Lorsque vous configurez la prise en charge de la séparation de domaine, vous pouvez ajouter une logique de domaine à cette nouvelle table Propriétés de l'application. Cette table peut contenir des propriétés qui n'existent pas dans la table Propriétés système. Vous pouvez également ajouter des propriétés à la table de configuration qui peuvent remplacer toute propriété que vous sélectionnez dans la table Propriétés système.

Par exemple, supposons que vous souhaitiez configurer une application avec une fonctionnalité Premier jour de la semaine. Parfois, vous voudrez peut-être que le premier jour de la semaine soit le dimanche. Dans d'autres cas, vous voudrez peut-être que le premier jour de la semaine soit le lundi. Dans la table du système de base, il n'y a peut-être qu'une seule option Jour 1, qui est le dimanche. Avec la nouvelle table, vous pouvez stocker une autre propriété, ce qui fait le jour 1, le dimanche, et un domaine enfant, le lundi.

Cette figure montre comment le système extrait les propriétés de la table Propriétés de l'application avant d'accéder à la table Propriétés système [sys_properties].



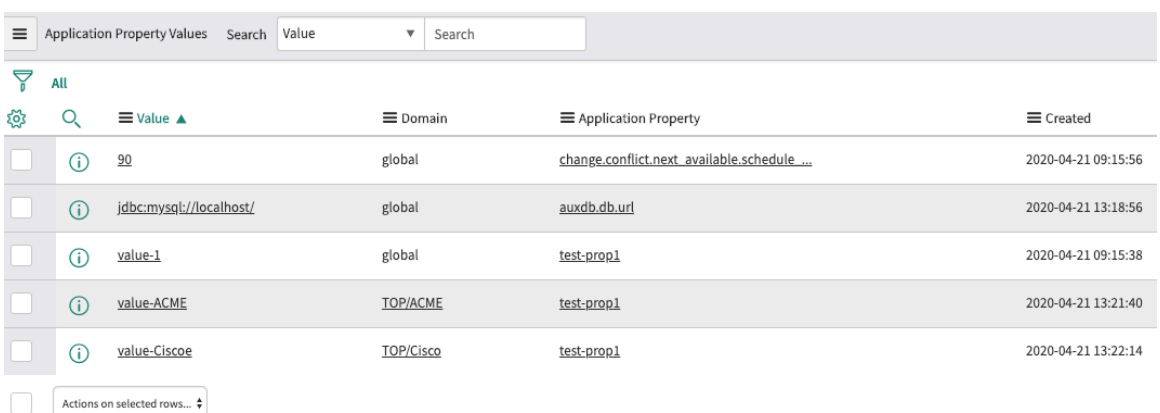
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement des applications incluses dans le périmètre dans la nouvelle table

La nouvelle table Propriétés de l'application est prise en charge à partir des applications incluses dans le périmètre. Le nom de propriété de l'application, similaire au nom de la propriété système, est unique, ce qui signifie qu'il est précédé du nom du périmètre s'il n'est pas global. Le périmètre d'une application a un impact sur votre configuration. Le champ d'application peut déterminer quel jour 1 est défini comme dimanche et lequel comme lundi. Vous pouvez utiliser la même propriété, mais la personnaliser de sorte que Jour 1, dimanche est le domaine parent et Jour 1, lundi est le domaine enfant. Dans la nouvelle table, il existe une colonne Domaine et une colonne Périmètre, de sorte que vous pouvez définir ces propriétés pour chacune.

Vous pouvez utiliser la vue Développer le champ d'application de domaine dans la table sys_application_property_value pour afficher tous les remplacements, comme illustré dans l'image suivante.



Remarque :

Si ces tables ne sont pas disponibles, assurez-vous d'avoir activé le module d'extension Domain Extension Installer (com.glide.domain.msp_extensions.installer).

Nouvelles tables de propriétés de l'application

La nouvelle table Propriétés de l'application système [sys_application_property] contient les champs suivants :

- nom
- description
- Type (choix de chaîne, vrai/faux, nombre entier, fuseau horaire, couleur, etc.)
- default_value
- propriété (référence à sys_properties)
- usage_notes
- read_roles
- write_roles
- Clé unique : (nom)

La nouvelle table Valeur de propriété de l'application système [sys_application_property_value] contient les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sys_application_property (réf. à sys_application_property)
- sys_domain
- sys_overrides
- valide
- Clé unique : (sys_application_property, sys_domain)

Nouvelles API

Les nouvelles API sont également prises en charge dans les applications incluses dans le périmètre. Les propriétés d'application séparées par domaine ont des API distinctes. L'API GlideApplicationProperty dispose de deux nouvelles méthodes scriptables, disponibles dans les applications globales et dans le champ d'application. Consultez GlideApplicationProperty : étendu, global pour en savoir plus sur ces nouvelles API.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Outil de migration de domaine

Utilisez l'outil de migration de domaine pour déplacer un client d'un environnement séparé par domaine vers sa propre instance dédiée.

Module d'extension Domain Migration Tool

Le module d'extension Domain Migration Tool (com.glide.domain.migration_tool) simplifie la tâche de déplacement d'un client d'un environnement séparé par domaine vers une instance dédiée plus flexible. Les clients peuvent vouloir migrer vers une instance distincte pour tirer davantage parti des ServiceNow AI Platform options. Bien que le module d'extension Séparation en domaines soit installé, les propriétés de séparation des données et des processus sont désactivées.

Remarque :
Vous devez demander une instance clonée et demander l'activation du module d'extension Outil de migration de domaine avant de pouvoir l'utiliser.

L'outil de migration de domaine s'exécute uniquement si la séparation des données et la séparation des processus sont activées dans l'instance séparée par domaine :

- La `glide.sys.domain.partitioning` propriété des données doit être définie sur **vrai**.
- La `glide.sys.domain.delegated_administration` propriété du processus doit être définie sur **true**.

Fonction de l'outil de migration

- Automatise une grande partie du processus de migration, en particulier le nettoyage des données.
- Migre l'instance séparée par domaine vers une nouvelle instance dédiée.
- Supprime les données de l'instance dédiée.

Remarque :
L'outil ne supprime pas les données globales, dans le domaine cible ou dans des domaines de données supplémentaires (si spécifié).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réduit les données de processus ou, s'il est impossible de les réduire, supprime les données de processus
- Conserve les enregistrements de processus visibles par le domaine cible
- Met à jour les tables sys_choice, sys_ui_list et sys_ui_related_list spéciales
- Nettoie les enregistrements ajoutés par les modules d'extension de séparation de domaine :
  - Règles métier
  - Actions d'interface utilisateur
  - Travaux planifiés
  - Sorties d'installation
  - Modules de navigation
- Désactive la séparation de domaine et supprime les domaines de l'instance clonée :
  - Définit ces propriétés sur **faux** dans l'instance clonée :
    - *`glide.sys.domain.partitioning`*
    - *`glide.sys.domain.delegated_administration`*
    - *`glide.sys.domain.enabled`*
  - Supprime tous les domaines, à l'exception du domaine cible et de tous les domaines de données spécifiés supplémentaires.
- Met à jour le champ **État** dans la table domain_migration_tool_status.

État individuel des tables

Statut	Description
En attente	État par défaut des tables séparées par domaine pendant la migration. La migration des tables est planifiée, mais n'a pas encore démarré la migration.
Échec	Échec au niveau de la table. Si le processus de migration se termine avec des erreurs, cet état indique quelles tables comportent des erreurs.
En cours d'exécution	État de la table en cours de migration. Une seule table peut avoir cet état et est en cours de migration.
Réussi	État des tables qui ont migré avec succès.
Terminé avec succès	Le processus de migration se termine sans erreur.
Terminé avec erreurs	Le processus de migration s'est terminé avec des erreurs.

- Consigne la progression et l'état sur syslog_domain

  La source est **MigrationTool** pour toutes les entrées de journal associées à la migration.
  - Consigne chaque table de données et le nombre de tables de données restantes
  - Journalise chaque table de processus et les enregistrements de domaine qui sont en cours de désactivation ou de suppression

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce que l'outil de migration ne fait pas

- Cloner l'instance
- Créer une autre instance séparée par domaine
- Migrer les enregistrements (données ou processus) si les propriétés de séparation des données ou des processus sont désactivées avant d'exécuter l'outil
- Modifier toutes les données sur l'instance source
- Supprimer les données globales, dans le domaine cible ou dans d'autres domaines de données (si spécifié)

Ce que vous devez faire après avoir exécuté l'outil

L'outil de migration de domaine automatise la suppression des données en dehors des domaines souhaités (le domaine cible, tous les domaines de données supplémentaires et le domaine global). Vous devez évaluer toutes les configurations restantes pour vous assurer qu'elles sont appropriées et fonctionnent pour votre instance dédiée. Par exemple, si vous aviez une règle métier qui définissait le champ de domaine sur les enregistrements, vous devriez peut-être désactiver cette règle métier car elle ne sert plus à rien.

Migrer une instance séparée par domaine vers une instance dédiée

Déplacez un client d'un environnement séparé par domaine vers son propre environnement d'instance dédié.

Avant de commencer

Rôle requis : admin

Procédure

1. Élever au rôle de security_admin.
   Consultez Accéder à un rôle privilégié pour en savoir plus.
2. Accédez à la **Tous** > **Administrateur de domaine** > **Outil de migration de domaine**.
   Accédez également avec **domain_migration_tool_status.list**.
3. Cliquez sur **Nouveau**.
4. Complétez le formulaire.

Champ	Description
Domaine cible	Spécifiez le domaine utilisé pour le processus et les données que vous souhaitez migrer. Seul le domaine cible est conservé, et non aucun de ses enfants, sauf indication contraire dans le champ **Domaines de données supplémentaires** .
Domaines de données supplémentaires	Vous pouvez également spécifier tous les domaines de données supplémentaires que vous souhaitez migrer. Si vous souhaitez migrer le domaine cible et tous ses enfants, vous devez spécifier tous les enfants.

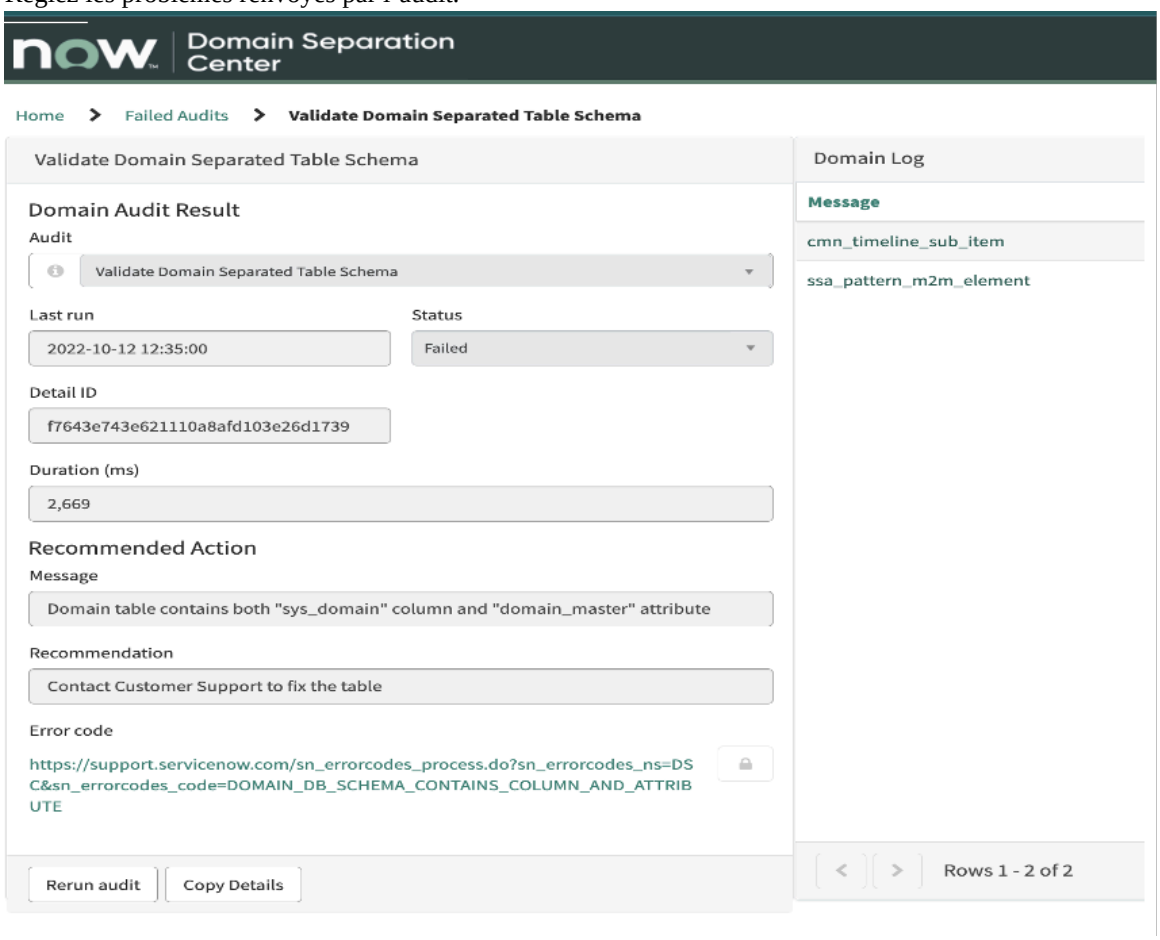
5. Sélectionnez **Soumettre**.
6. Ouvrez le formulaire que vous venez de soumettre.
7. Accédez à la **Tous** > **Centre Séparation en domaines** > **Configurer des audits** .
   Consultez Centre Séparation en domaines pour plus d'informations.
8. Définissez l'audit **Valider le schéma de tables séparées par domaine** sur **Actif** et affectez un calendrier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il s’agit d’un audit de domaine de précaution qui permet de vérifier au préalable l’intégrité des tables séparées par domaine du schéma. Cela vous permet de corriger les erreurs avant d’exécuter la migration.

9. Exécutez le **calendrier d’audit** qui inclut le schéma.
   Consultez Exécuter immédiatement les audits pour en savoir plus.
10. Réglez les problèmes renvoyés par l’audit.

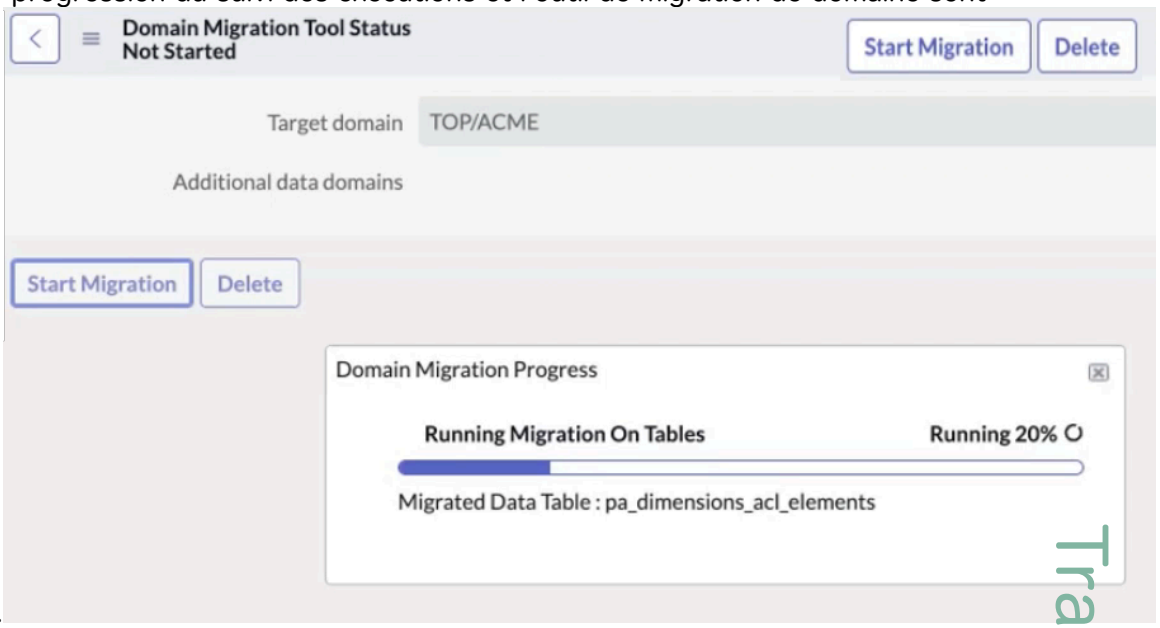


11. Sélectionnez **Démarrer la migration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La barre de progression du suivi des exécutions et l'outil de migration de domaine sont déclenchés.



- La table de migration en cours s'affiche avec le pourcentage total de tables migrées avec succès.
- Table dans laquelle toutes les tables séparées par domaine sont enregistrées avec l'état de migration, le nombre total d'enregistrements dans chaque table et le nombre d'enregistrements migrés.
- Le nombre de tables où la migration a échoué est également enregistré.
- **L'état** est mis à jour au fur et à mesure que l'outil exécute ses fonctions.
- La migration de domaine est toujours en cours d'exécution en arrière-plan si vous fermez la barre de progression. Accédez à la table `sys_execution_tracker` et recherchez **Migration en cours sur tables** pour vérifier que le processus de migration s'exécute en arrière-plan.

L'état de l'outil de migration de domaine affiche les champs suivants :

Champs d'état de l'outil de migration de domaine

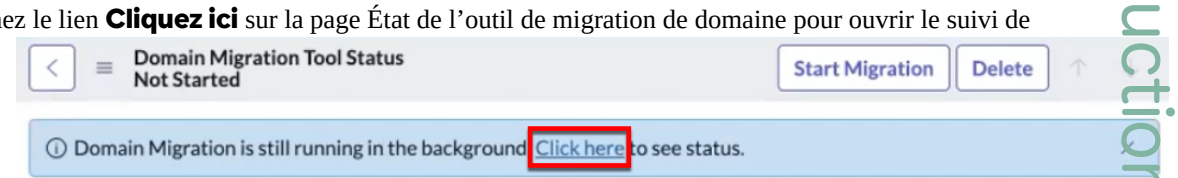
Champ	Description
Statut	Affiche l'état de la migration. ○ **Migration des tables de données en cours.** ○ **Migration réussie** : état mis à jour après une migration réussie. ○ **Une mauvaise configuration est observée sur l'une des tables séparées par domaine** : Indique un échec de la migration des données. Une erreur de schéma a été trouvée, la migration ne démarre pas. Exécuter l'audit **Valider le schéma de table séparée par domaine**. L'audit échouera et affichera les tables qui ne suivent pas la norme de schéma. ○ **Terminé avec des erreurs dans les tables de revisite** : le nombre de tables pour traiter la migration des schémas est répertorié. Localisez les défaillances dans le décompte des tables de revisite et résolvez les problèmes de schéma.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

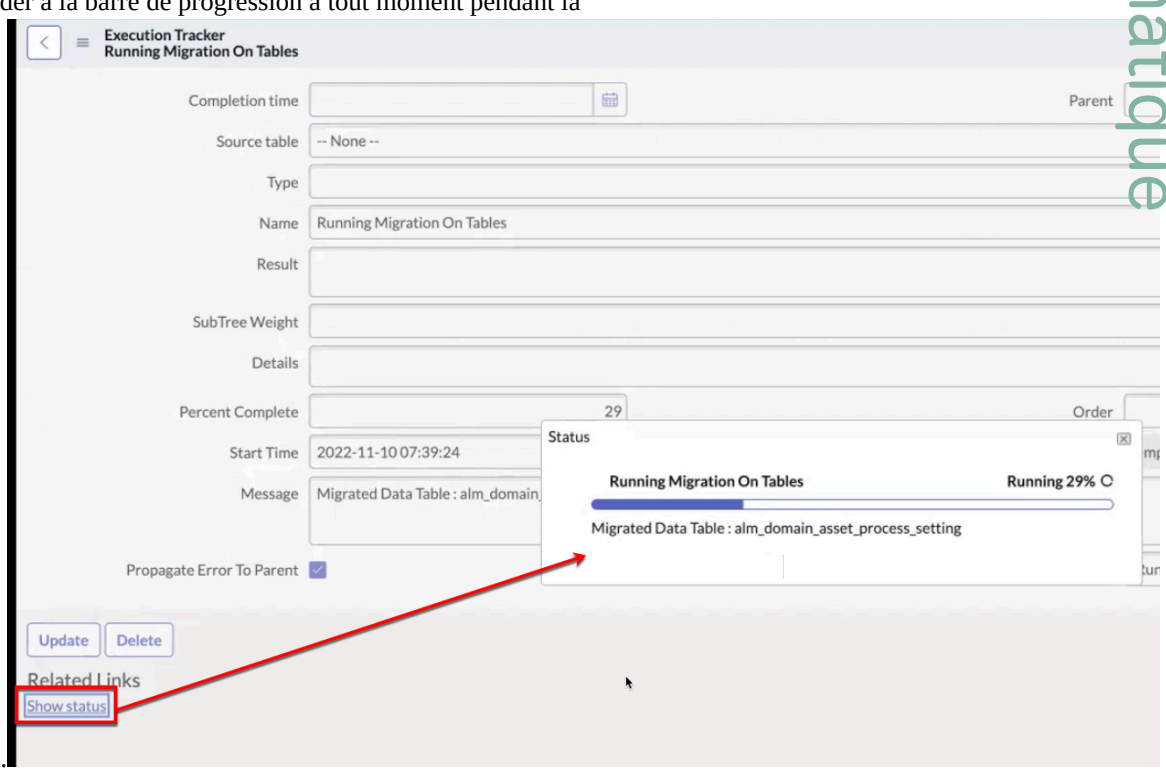
Champ	Description
	○ **Échec de la migration de domaine pour les tables...** : les enregistrements non cibles doivent être supprimés manuellement des tables ayant échoué. ○ **Terminé avec succès** : lorsque toutes les tables ont migré.
Domaine cible	Domaine cible sélectionné pour la migration.
Domaines de données supplémentaires	Indique si plusieurs domaines de migration ont été sélectionnés.
Nombre des tables de revisite	Ce champ se remplit uniquement si la migration d'une table échoue. S'il n'y a pas d'échec, ce nombre est égal à zéro. Dans ce cas, les tables seront revisitées pour retenter la migration. En l'absence d'échecs, il n'est pas nécessaire de revoir les tables ou de retenter la migration.
Table de progression actuelle	Affiche le nom de la table en cours de migration. Une fois la migration réussie, ce champ est vide.

12. Sélectionnez le lien **Cliquez ici** sur la page État de l'outil de migration de domaine pour ouvrir le suivi de l'exécution.



Vous pouvez également accéder à la table `sys_execution_tracker` et rechercher **Running Migration on Tables** pour vérifier l'exécution du processus de migration en arrière-plan.

13. Sélectionnez **Afficher l'état** dans la section Liens connexes pour accéder à la barre de progression à tout moment pendant la migration.



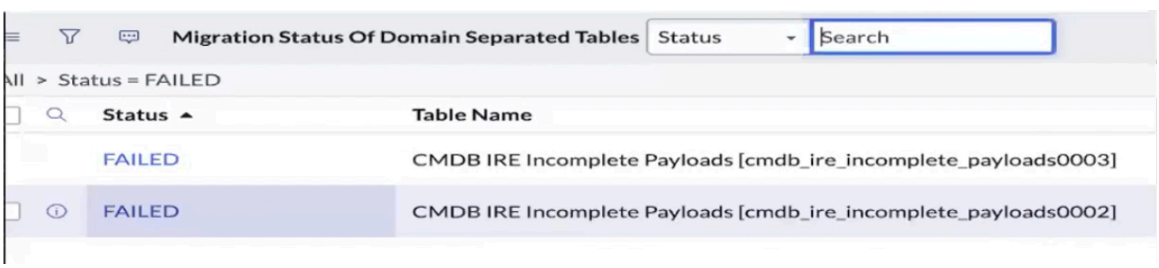
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

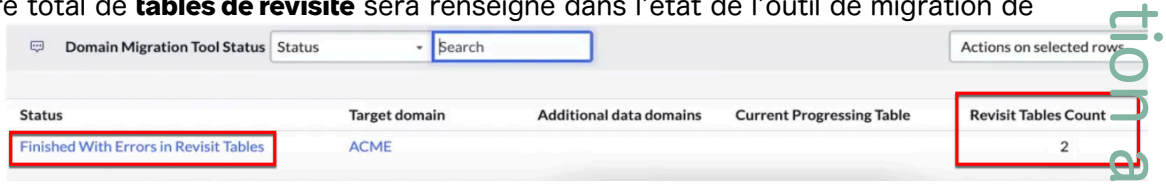
Si une table échoue à la vérification du schéma, l'état global de migration des tables séparées par domaine est **défini sur Échec**.



Il y aura des entrées **ayant échoué** pour chaque table correspondante.



Le reste de la migration se poursuit et un résumé de toutes les tables ayant échoué et du nombre total de **tables de revisite** sera renseigné dans l'état de l'outil de migration de domaine.



L'état est **défini sur Terminé avec succès** lorsque la migration est terminée.



Administration des processus

L'administration des processus permet aux administrateurs de définir des stratégies spécifiques à un domaine.

Les politiques définies plus bas dans la hiérarchie de domaine remplacent les politiques définies plus haut dans la hiérarchie de domaine. Lorsqu'ils sont dans un domaine, les administrateurs peuvent définir des versions spécifiques au domaine de ces stratégies et paramètres globaux :

- Scripts clients
- Politiques système
- Noms de l'application et du module

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rôles d'application
- Filtres de module

⚠ Avertissement :
Tous les utilisateurs disposant du rôle admin bénéficient d'un accès spécial à toutes les fonctionnalités, fonctions et données système, car les administrateurs peuvent remplacer les règles ACL et subir avec succès toutes les vérifications de rôles. Accordez ce privilège avec soin.

Lorsque les utilisateurs disposent du rôle **administrateur** , toutes les politiques de l'instance sont alors disponibles, quel que soit le domaine affecté. Ils peuvent entrer un domaine spécifique, et seules les politiques de ce domaine ou de domaines supérieurs sont visibles et traitées lors d'une transaction pertinente. Lorsqu'un administrateur modifie une politique qui se trouve dans un domaine supérieur ou le domaine global, le système crée automatiquement un nouvel enregistrement pour le domaine actuel de cet administrateur. Elle ne modifie pas l'enregistrement d'origine de la politique, de l'application ou du module. Ce nouvel enregistrement remplace l'original.

Pour apporter des modifications à une politique dans un domaine de niveau inférieur, accédez à ce domaine et modifiez-la. Cette approche crée l'enregistrement de politique dans votre domaine qui remplace l'enregistrement de politique de niveau supérieur d'origine.

Ne changez pas la stratégie de niveau supérieur, puis le champ **Domaine** de cette stratégie. Cette approche ne crée pas d'enregistrement de politique dans votre domaine de niveau inférieur et ne conserve pas l'enregistrement de politique pour le domaine de niveau supérieur.

Le champ **sys_overrides** indique qu'une politique, une application ou un module à un niveau inférieur de la hiérarchie remplace un enregistrement à un niveau supérieur. Le système définit automatiquement ce champ lorsqu'un administrateur tente de modifier une politique, une application ou un module appartenant à un autre domaine placé plus haut dans la hiérarchie.

Plutôt que de modifier l'enregistrement de niveau supérieur, la tentative de mise à jour est changée en insertion et le champ **sys_overrides** est défini pour indiquer la politique, l'application ou le module de niveau supérieur qui est remplacé. Ultérieurement, lorsque les enregistrements d'une transaction pertinente sont chargés, la politique, l'application ou le module spécifique au domaine de remplacement est utilisé à la place de l'original.

Domaines pour l'administration des processus

Par défaut, l'administration des processus utilise toujours le domaine de l'enregistrement pour déterminer les politiques à appliquer.

Le domaine de l'enregistrement a priorité sur le domaine de l'utilisateur. S'il n'existe aucune politique dans le domaine de l'enregistrement, l'administration déléguée recherche les politiques au niveau immédiatement supérieur de la hiérarchie de domaine. La recherche de politiques de domaine se poursuit dans la hiérarchie des domaines jusqu'au domaine global. En l'absence de politiques de domaine à un niveau inférieur dans la hiérarchie des domaines, l'administration des processus utilise les politiques du domaine global.

Par exemple, Fred Luddy est un utilisateur du domaine Acme qui peut voir les enregistrements dans les domaines enfants des domaines enfants Acme : Atlanta, Acme : San Diego et Acme : NY. Lorsque cet utilisateur ouvre un enregistrement dans le domaine Acme : San Diego, l'administration du processus vérifie d'abord les politiques dans le domaine Acme : San Diego. S'il n'existe aucune politique à ce niveau de la hiérarchie de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

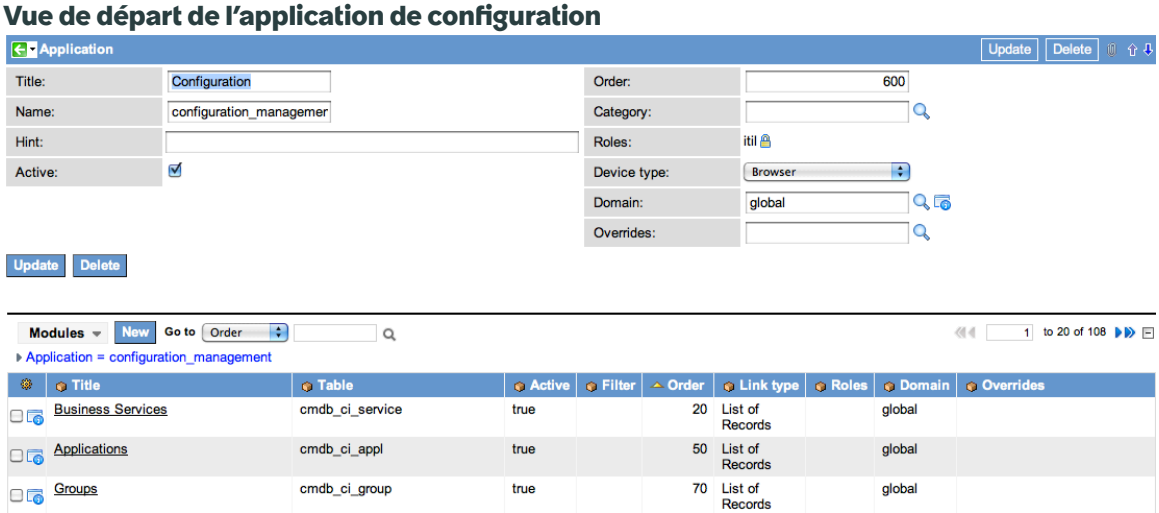
domaine, l'administration des processus recherche des politiques provenant du domaine ACME. Si le domaine ACME n'contient aucune politique, l'administration des processus utilise les politiques de domaine globales, car il n'existe aucun autre domaine placé plus haut dans la hiérarchie des domaines.

Exemple d'administration de processus avec des applications spécifiques au domaine

L'exemple suivant illustre l'administration des processus avec des applications et des modules spécifiques au domaine.

En tant qu'administrateur du domaine océanique, David Loo décide de personnaliser l'application Configuration. Pour commencer, David passe en revue les modules disponibles dans le module de l'application Configuration.

Vue de départ de l'application de configuration



David décide de renommer l'application de configuration en CMDB et de permettre au rôle inventory_admin de voir l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de modifications spécifiques au domaine apportées à l'application de configuration

Applications | New | Go to Title | 1 to 20 of 46

All > Active = true > Device type != Mobile

Title	Active	Order	Roles	Name	Domain	Overrides
Asset Management	true	900	asset	asset	global	
BSM Map	true		admin itil	bsm_map	global	
Change	true	400	itil	change_management	global	
CMDB	true	600	itil inventory_admin	configuration_management	Database	configuration_management
Content Management	true		content_admin	cms	global	
Contract Management	true	1,000	asset contract_manager	asset_contracts	global	
Domain Admin	true		domain_admin	domain_admin	global	
ECC	true		admin	ecc	global	
Homepage Admin	true		admin	home	global	
Incident	true	200	itil	incident_management	global	
Instance Clone	true		clone_admin	instance_clone	global	
Knowledge Base	true	800	knowledge	km	global	
Metrics	true		itil_admin metric_admin	metrics	global	
MID Server	true		admin	MID	global	
Organization Management	true	875	asset	organization_management	global	
Problem	true	300	itil	problem_management	global	
Reports	true	1,100	itil	reports	global	
SAML 2 Single Sign-on	true		admin	saml_2_single_sign_on	global	
SAML Single Sign-on	true		admin	SAML Single Sign-on	global	

Activate | Deactivate | Actions on selected rows... | 1 to 20 of 46

Ensuite, David décide de changer l'application Incident en activant le module **Ouvert - dans l'état « Nouveau »** et en ajoutant un nouvel élément de filtre pour afficher les incidents ouverts dans la catégorie Océanique.

Exemples de changements spécifiques au domaine apportés au module Ouvrir - « Nouveau » état

Module | = Required field | Update | Delete

Title:	Open - in "New" state	Link type:	List of Records
Table:	Incident [incident]	View name:	
Order:	200	Roles:	
Application:	incident_management		
Hint:			
Active:	☑		
Image:			

Filter:

	Incident state	is	New
and	Active	is	true
and	Category	is	Database

Arguments:

```
incident_state=1^active=true
```

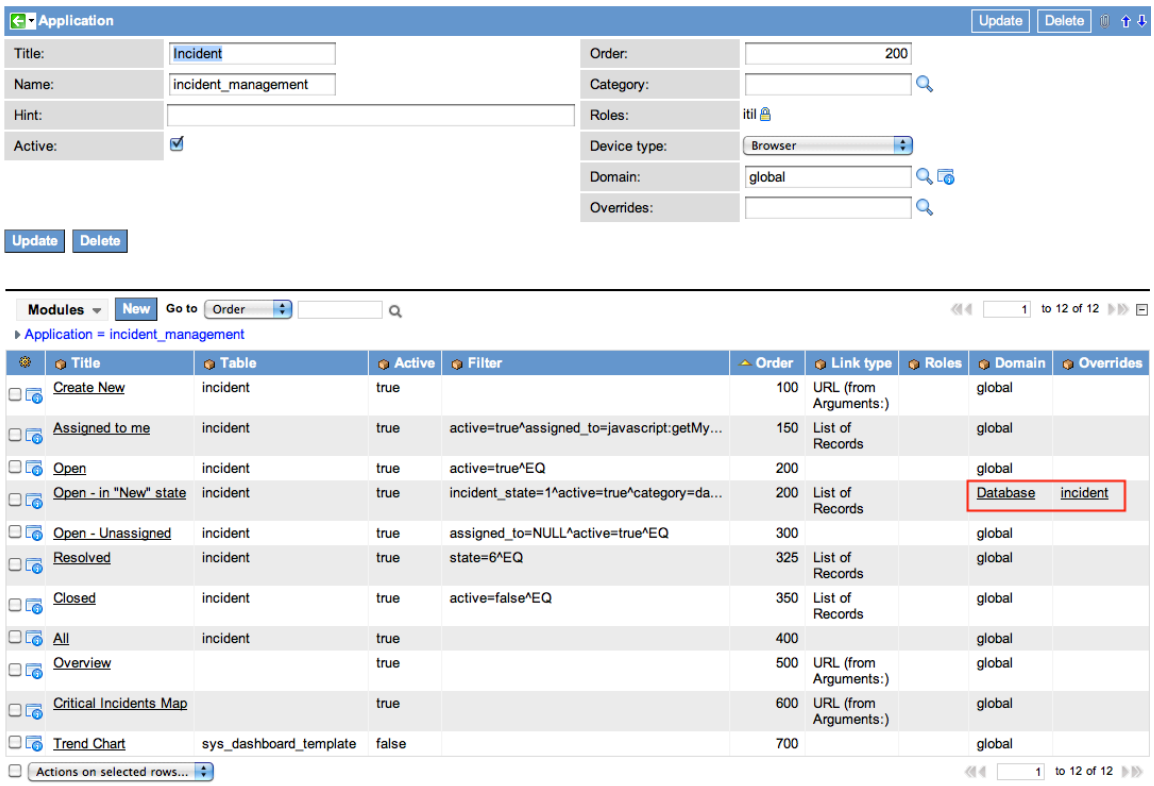
Update | Delete

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

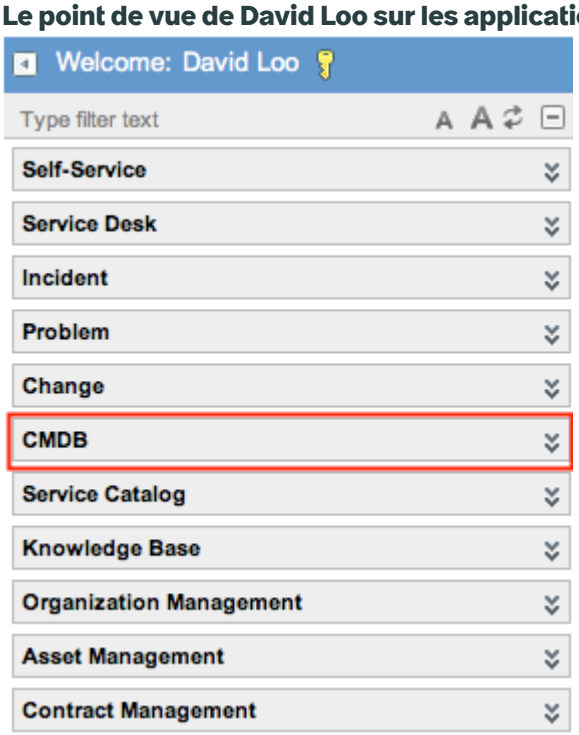
Cela crée une nouvelle entrée de module dans l'application plutôt que d'écraser le module existant dans le domaine global.

Vue de l'application Incident spécifique au domaine



Si un autre administrateur d'un autre domaine, tel que Fred Luddy, se connecte et consulte l'application Configuration, les paramètres du domaine global s'affichent.

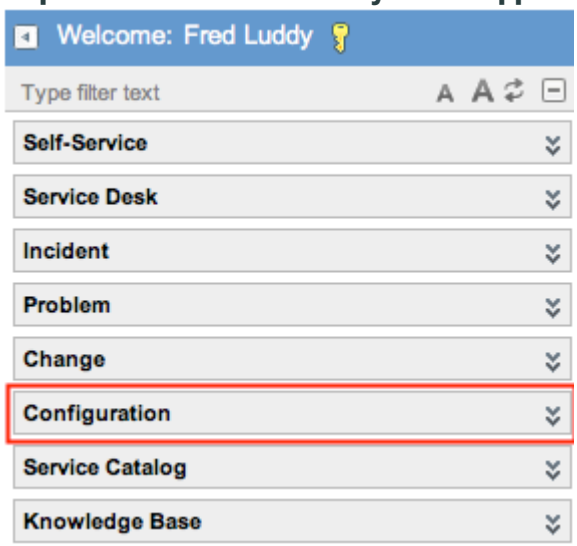
Le point de vue de David Loo sur les applications



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le point de vue de Fred Luddy sur les applications



Activer la connexion de domaine documentée et les messages de débogage

Les journaux de domaine et les messages de débogage vous permettent de résoudre les erreurs de configuration de domaine.

Avant de commencer

Rôle requis : admin

Assurez-vous que vous êtes la dernière instance pour de meilleures performances.

Procédure

1. Dans Centre Séparation en domaines, accédez à **Administrateur de domaine**.
2. Cliquez sur **Configurer le centre du domaine**.
3. Pour **Activer la journalisation de domaine détaillée**, cochez la case **Oui** .
4. Cliquez sur **Mettre à jour**.

Afficher un message de domaine en temps réel

Vous pouvez afficher les messages de domaine en temps réel à partir des journaux système.

Avant de commencer

Rôle requis : admin

Procédure

1. Activer la journalisation de domaine détaillée : Accédez à **Tous** > **Administrateur de domaine** > **Centre Séparation en domaines** > **Configurer le centre du domaine** > **Active la journalisation dans le domaine des détails** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **Vrai**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
   Comme il s'agit d'un examen en temps réel, il n'est pas nécessaire de laisser la session de débogage s'exécuter avant de vérifier les fichiers journaux.
3. Accédez à la console de débogage de session pour afficher les journaux de domaine système détaillés.
4. Rechercher le texte Requête par rapport à la table.

   Cette requête trouve les messages du journal au format suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
08:36:43.974: [Domain Paths] Query against table incident restricted by domain values
 [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

Dans cet exemple, l'utilisateur affichant la table Incident n'a vu que les enregistrements qui correspondaient aux domaines Base de données Atlanta, Base de données, Base de données San Diego, global et NY DB.

Afficher un message de domaine historique

Affichez les messages de domaine historiques dans le fichier journal pour résoudre les problèmes de séparation de domaine.

Avant de commencer

Rôle requis : admin

Procédure

1. Activer la journalisation de domaine détaillée : Accédez à **Tous** > **Administrateur de domaine** > **Centre Séparation en domaines** > **Configurer le centre du domaine** > **Active la journalisation dans le domaine des détails** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **Vrai**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
3. Laissez la session de débogage s'exécuter pendant une période, par exemple une journée, avant de vérifier les fichiers journaux.
4. Accédez à la **Journaux système** > **Utilités** > **Téléchargement du fichier journal de nœud**.
5. Ouvrez l'enregistrement du jour que vous souhaitez afficher.
   Les fichiers journaux utilisent le format de dénomination localhost_log.<aaaa-mm-jj>.txt.
6. Cliquez **sur le lien** connexe Télécharger le journal.
7. Ouvrez le fichier journal téléchargé dans un éditeur de texte et recherchez les messages du journal avec le format suivant :

   Requête par rapport à la table Incident restreint par des valeurs de domaine [global, Software[8a4dde73c6112278017a6a4baf547aa7]]

   Dans cet exemple, un utilisateur a uniquement vu les enregistrements de la table Incident qui correspondaient aux domaines global et logiciel.

Résoudre les erreurs de séparation de domaine

Si vous rencontrez des problèmes de séparation de domaine, consultez cette liste de solutions.

Erreur ou symptôme	Solution
Un domaine sys_id pointe vers un domaine qui n'existe pas	Cette erreur se produit lorsqu'un enregistrement de données, tel qu'un enregistrement d'utilisateur ou de tâche, a une valeur de colonne sys_domain dont le sys_id n'existe pas dans la table de domaine actuel. Le sys_id de domaine peut avoir été supprimé accidentellement ou il peut faire référence à une table de domaine précédente si vous avez modifié la table de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreur ou symptôme	Solution
	Pour corriger l'erreur, ouvrez une liste pour la table contenant l'erreur, filtrez sur la valeur de sys_domain non valide. Ensuite, saisissez manuellement la valeur sys_domain correcte ou supprimez-la. **Remarque :** Vous pouvez avoir des sys_ids de domaine non valides dans n'importe quelle table qui fait référence à la table de domaine. Par exemple, des ID de domaine non valides peuvent apparaître dans les tables Domaine de visibilité utilisateur [sys_user_visibility], Domaine de visibilité de groupe [sys_user_group_visibility] et Domaine contenu [domain_contains].
Un chemin de domaine ou un numéro de domaine sys_id pointe vers le mauvais domaine	Cette erreur se produit lorsqu'une requête de numéro de domaine ou de chemin de domaine n'est pas synchronisée avec le nom de domaine réel. Cette erreur peut se produire avec les numéros de domaine lorsque l'ajout de domaines nécessite une renumérotation ou lors de la conversion de numéros de domaine en chemins de domaine. Pour corriger l'erreur, vérifiez les résultats dans le Centre Séparation en domaines fichier . Si l'erreur persiste, vous pouvez modifier manuellement la valeur des colonnes sys_domain_path ou sys_domain_number pour pointer vers le domaine approprié.
L'arborescence du domaine est corrompue	Cette erreur se produit s'il existe une série de relations de domaine qui créent une boucle infinie entre les domaines. Pour corriger l'erreur, ouvrez une liste pour la table de domaine et modifiez manuellement les valeurs du domaine contient pour ne pas former une boucle.

Utilitaire d'activation de séparation en domaines en post-production

L'utilitaire d'activation de séparation en domaines en post-production facilite l'activation de la séparation en domaines dans un environnement de production.

Module d'extension Post-production Domain Separation Activation Utility

Le module d'extension Post-Production Domain Separation Activation Utility (com.glide.domain.activation_utility) simplifie la création d'un environnement séparé par domaine dans un environnement de post-production. Les clients peuvent activer Domain Separation sur les environnements de post-production pour tirer davantage parti des ServiceNow AI Platform fonctionnalités. L'utilitaire fournit une configuration guidée étape par étape pour la création de domaines.

Remarque :
Le processus de remplissage des enregistrements de domaine dans des tables séparées par domaine nécessite un temps d'arrêt ou un accès restreint à l'instance.

Fonction de l'utilitaire d'activation

- Fournit une configuration guidée étape par étape pour la création de domaines.
- Exécute une tâche en arrière-plan pour gérer l'installation de Séparation de domaine avec les propriétés de processus et de séparation des données désactivées.
- Conserve les enregistrements de processus visibles par le domaine cible (en premier)
- Détecte, identifie et consigne les erreurs pendant le processus de création de domaine

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Présente des résolutions pour les erreurs courantes
- Consigne toutes les actions effectuées pendant le processus de configuration à des fins d'audit
- Génère un résumé détaillé, comprenant toutes les actions effectuées, les domaines créés et tous les changements apportés au système

Gestion des tâches du domaine

Mettez en file d'attente plusieurs mises à jour de Domain Separation séquentiellement dans une seule tâche en arrière-plan à l'aide du gestionnaire de tâches de domaine.

Lorsqu'un enregistrement de domaine est modifié, comme un changement de parent ou un changement de hiérarchie, par défaut, une tâche s'exécute pour corriger tous les enregistrements dans des tables séparées par domaine. Vous pouvez contrôler quand ce comportement se produit avec le **gestionnaire de tâches du domaine** et surveiller la progression de la tâche en cours avec le bouton Afficher la progression de la **tâche** .

Utilisez le **Gestionnaire de tâches de domaine** pour mettre en pause les tâches de domaine, mettre en file d'attente plusieurs changements de table de domaine et déclencher la tâche en file d'attente lorsqu'elle est prête avec tous les changements.

Progression de la tâche de domaine

Étiquette	Description
Type de tâche	Type de tâche actuel
Statut	Pour l'état de la tâche, voir État de la **tâche** dans le gestionnaire de tâches pour plus d'informations.
Progression	Progression de la tâche en cours

Gestionnaire de travaux du domaine

Champ	Description
Type de tâche	Types de tâches d'assistance : Changement de hiérarchie
État de la tâche	• Actifs • En pause **Remarque :** Par défaut, les tâches en pause reprendront automatiquement dans 1 heure. Cochez cette option pour désactiver cette option et activer manuellement la tâche ultérieurement

Supprimer par domaine

Nettoyez les domaines de niveau feuille inactifs dans la hiérarchie des domaines à l'aide d'un outil contrôlé et automatisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur de séparation de domaine

Procédure

1. **Tous** > **Administrateur de domaine** > **File d'attente de nettoyage**
2. Sélectionnez le bouton Préparer pour le **nettoyage** .
3. Sélectionnez les domaines à mettre en file d'attente pour suppression.
   La liste affiche tous les domaines de niveau feuille inactifs disponibles qui peuvent être sélectionnés pour suppression.
4. Sélectionnez **Enregistrer**.
   Les domaines sélectionnés refléteront désormais un état **Prêt pour l'étape intermédiaire** dans la table. Les domaines doivent être intermédiaires avant d'être mis en file d'attente pour suppression.
5. Sélectionnez le bouton **Passer à l'étape intermédiaire** .
6. Saisissez le nombre de jours de conservation du domaine intermédiaire avant sa suppression.

Remarque :
Une fois que le domaine est passé à l'état **Intermédiaire et Suppression planifiée** , il ne peut pas être supprimé de la file d'attente de nettoyage.

Avant qu'un domaine ne soit supprimé, les administrateurs de domaine peuvent accéder à l'empreinte de données du domaine.

7. Sélectionnez le bouton **Prévisualiser les données de domaine** .
   Une tâche sera mise en file d'attente pour analyser les domaines inactifs à la recherche de métadonnées.
8. Une fois la tâche exécutée, sélectionnez un enregistrement de domaine pour afficher ses métadonnées.

Centre Séparation en domaines

Auditez régulièrement vos domaines pour révéler les problèmes.

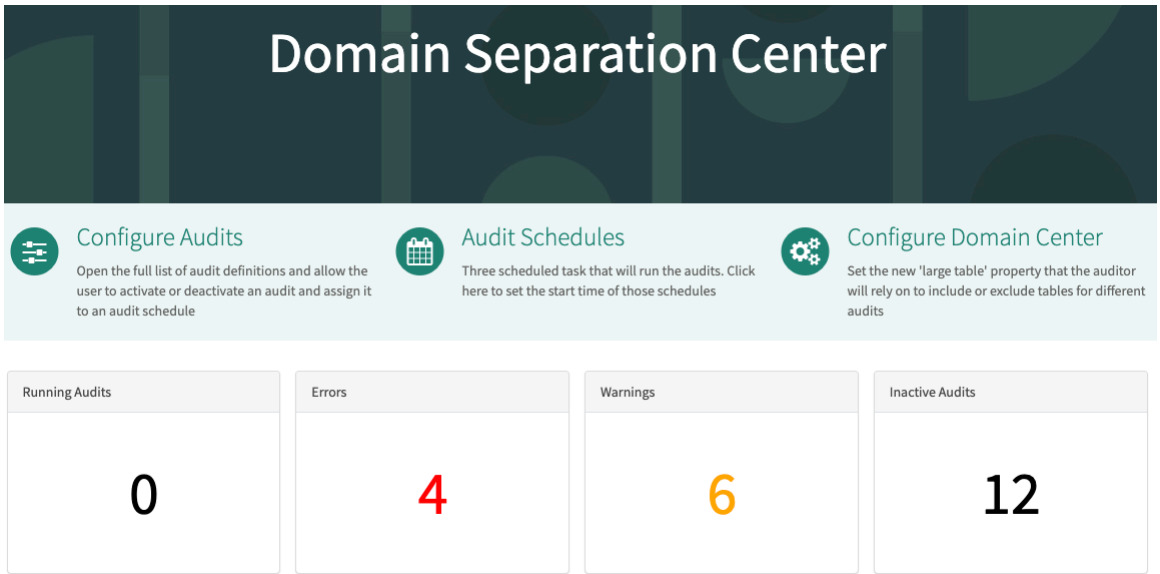
Vue d'ensemble

Le centre Séparation en domaines est un tableau de bord dans lequel vous pouvez planifier et configurer des audits pour tous les domaines stockés dans votre table domain_audit_definition. Le tableau de bord vous permet d'examiner les résultats d'audit et d'approfondir les erreurs et les avertissements de domaine. Vous pouvez trouver le tableau de bord du centre Séparation en domaines à l'adresse <ServiceNow-instance-name>/domaincenter.

Le Centre de séparation en domaines fournit de nombreux audits. Vous ne pouvez pas créer le vôtre. Vous pouvez toutefois configurer leur fréquence. Les audits s'exécutent sur tous les domaines stockés dans la table domain_audit_definition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer les audits

Vous pouvez spécifier si un audit est actif et à quelle fréquence il s'exécute.

1. Dans le Centre Séparation en domaines, sélectionnez **Configurer les audits**.

   La page **Configurer les audits** s'affiche.

2. Configurez chaque audit que vous souhaitez rendre actif. Les audits sont inactifs par défaut.
   a. Sélectionnez un audit.
   b. Cochez la case **Actif** pour activer l'audit.
   c. Spécifiez la fréquence d'exécution de l'audit dans le champ **Fréquence** .

      Le centre Séparation en domaines exécute tous les audits marqués avec la même fréquence en même temps. Ne sélectionnez pas **Quotidien** pour les audits qui s'exécutent sur des tables volumineuses.

   d. Répétez ces étapes pour chaque audit que vous souhaitez activer.
3. Sélectionnez **Enregistrer**.

Calendriers d'audits

Configurez un ou plusieurs audits à exécuter quotidiennement, hebdomadairement ou mensuellement. Le planificateur spécifie les jours et les heures d'exécution de ces audits. Tous les audits avec la même fréquence de planification s'exécutent séquentiellement en tenant compte de l'heure que vous configurez.

1. Dans le centre Séparation en domaines, sélectionnez **Calendriers d'audit**.

   La page **Calendrier d'audit** s'affiche.

2. Configurez les calendriers d'audit.
   a. Sélectionnez un nom de calendrier.
   b. Spécifiez l'heure de la journée à laquelle exécuter l'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les unités de temps sont mesurées avec l'horloge de 24 heures, c'est-à-dire que 14 équivaut à 14 heures.

c. Pour les calendriers hebdomadaires, sélectionnez le jour de la semaine pour exécuter l'audit, où 1 est le dimanche.

d. Pour les calendriers mensuels, sélectionnez le jour du mois pour exécuter l'audit.

e. Répétez la procédure pour les autres calendriers.

3. Sélectionnez **Enregistrer** pour enregistrer les changements de configuration.
4. Sélectionnez **Exécuter maintenant** pour exécuter tous les audits planifiés à la fréquence indiquée en haut du volet droit, par exemple, si le titre du volet est **Calendrier d'audit du domaine : quotidien**, tous les audits qui s'exécutent quotidiennement sont exécutés.

Pour afficher l'état d'un audit en cours, dans le centre Séparation en domaines, sélectionnez le numéro dans la zone **Audits en cours** .

Exécuter immédiatement les audits

Les audits s'exécutent généralement comme prévu. Vous pouvez toutefois exécuter tous les audits sur commande.

1. Dans le centre Séparation en domaines, sélectionnez **Calendriers d'audit**.

   La page **Calendrier d'audit** s'affiche.

2. Sélectionnez le nom du calendrier d'audit que vous souhaitez exécuter (par exemple, quotidien, hebdomadaire ou mensuel).
3. Sélectionnez **Exécuter maintenant**.

Pour afficher l'état d'un audit en cours, dans le centre Séparation en domaines, sélectionnez le numéro dans la zone **Audits en cours** .

Configurer le centre Séparation en domaines

1. Dans Centre Séparation en domaines, sélectionnez Configurer le **centre du domaine**.
2. Sur la page **Configurer le centre du domaine** , pour **Active la journalisation de domaine détaillé,** sélectionnez **Oui** pour stocker des journaux détaillés qui aident à diagnostiquer les problèmes liés au domaine. Une journalisation détaillée peut entraîner des problèmes de performances.

   Ces journaux font référence aux journaux côté serveur dans la table syslog_domain. Pour plus d'informations sur l'affichage des journaux, voir Afficher les audits avec les avertissements et les défaillances.

3. Dans la zone de liste double, sélectionnez et déplacez toutes vos tables volumineuses dans la colonne **Sélectionné** .

   Les audits quotidiens ne doivent pas s'exécuter sur des tables volumineuses. Les noms de table grisés de la colonne **Sélectionné** sont volumineux et ne peuvent pas être déplacés vers la colonne **Disponible** .

4. Sélectionnez **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les audits avec avertissements et échecs

Sur le tableau de bord, **Erreurs** et **avertissements fournissent des** informations détaillées sur les audits qui ont rencontré des problèmes. Les journaux associés à Séparation de domaine résident sur votre serveur dans la table syslog_domain.

1. Dans le centre Séparation en domaines, sélectionnez le numéro dans la zone **Erreurs** ou **Avertissements** .

   La page **Erreurs** ou **Avertissements** s'affiche respectivement.

2. Sélectionnez l'un des audits dans la liste.

   La page affiche des informations détaillées sur les problèmes liés à l'audit que vous avez sélectionné. Les messages dans **Détails des résultats d'audit** font référence aux valeurs de la table des syslog_domain pour les audits de table qui ont révélé des erreurs ou des avertissements.

3. Pour afficher les journaux sur le serveur qui fournissent des informations sur les audits d'avertissement ou d'erreur :
   a. Copiez la valeur **de l'ID de détail** dans le panneau de gauche d'un avertissement ou d'une erreur.
   b. Dans le navigateur de filtrage de HI, saisissez *`syslog_domain.do`*.

      La page Journal du domaine s'affiche.

   c. Dans le champ **de recherche Source** , entrez `=<Detail-ID >` (aucun espace après le signe égal), par exemple, =f6a00fd29a85b300a9503a81b9169678.

      La page Journal de domaine affiche uniquement les journaux associés à l'audit avec l'ID de détail que vous avez spécifié. Chaque ligne de la table spécifie un enregistrement différent dans lequel l'audit a trouvé des problèmes. Notez que le champ **Message** de cette page correspond aux valeurs affichées dans la colonne **Message** du centre de services de domaine. Le format du message correspond au type d'audit.

4. Sélectionnez :
   - **Réexécuter l'audit** : réexécutez un audit pour voir s'il rencontre toujours un avertissement ou une erreur.
   - **Désactiver l'audit** : désactiver un audit.
   - **Copier les détails** : copie les détails de l'audit dans le presse-papiers.

Afficher les audits en cours et en attente

Les audits actifs s'exécutent périodiquement ou sont mis en file d'attente pour s'exécuter comme prévu. Vous pouvez afficher leur état au fur et à mesure de leur exécution.

1. Sélectionnez le nombre dans la zone **Audits en cours** pour afficher les audits en cours d'exécution ou en attente d'exécution.

   La page **Audits en cours** s'affiche.

2. Sélectionnez un audit pour en savoir plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les audits inactifs

1. Sélectionnez le nombre dans la zone **Audits inactifs** .

   La page **Audits inactifs** affiche tous les audits actuellement désactivés.

2. Sélectionnez l'un des audits pour afficher plus d'informations à son sujet.
3. Pour activer un audit, cochez la case **Actif** et utilisez le champ **Fréquence** pour spécifier la fréquence d'exécution de l'audit.
4. Sélectionnez **Mettre à jour**.

Configurer le centre Séparation en domaines

Spécifiez quelles tables des domaines sont volumineuses et si vous souhaitez une journalisation détaillée.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier des audits sur une base quotidienne, hebdomadaire ou mensuelle. Les audits exécutés sur des tables volumineuses peuvent prendre beaucoup de temps. Pour cette raison, évitez d'exécuter des audits quotidiennement sur des tables volumineuses. Commencer un nouvel audit sur un audit qui prend plus d'une journée peut avoir des conséquences négatives.

Une journalisation détaillée peut fournir un meilleur aperçu des problèmes détectés lors des audits, mais peut entraîner des problèmes de performance.

Procédure

1. Dans Centre Séparation en domaines, sélectionnez Configurer le **centre du domaine**.
   La page Configurer le centre de domaine s'affiche.
2. Sélectionnez **Oui** pour **Active la journalisation de domaine détaillé** afin de stocker des journaux détaillés qui aident à diagnostiquer les problèmes liés au domaine.
   Ces journaux font référence aux journaux côté serveur dans la table Journal de domaine [syslog_domain]. Pour plus d'informations sur l'affichage des journaux, consultez la section Afficher les audits avec avertissements et défaillances.
3. Dans la liste, déplacez toutes vos tables volumineuses dans la colonne **Sélectionné** .
   Les audits quotidiens ne doivent pas s'exécuter sur des tables volumineuses. Les noms de table grisés de la colonne **Sélectionné** sont volumineux et ne peuvent pas être déplacés vers la colonne **Disponible** .
4. Sélectionnez **Mettre à jour**.
5. Si vous avez des tables volumineuses qui ne doivent jamais être auditées, définissez la `com.glide.domain.audit.big_tables.additional` propriété système sur une liste séparée par des virgules de ces noms de tables.

Configurer les audits

Configurez si un audit est actif et à quelle fréquence il s'exécute.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Configurer les audits**.
   T apparaît.
2. Sur la page Configurer les audits, configurez chaque audit que vous souhaitez rendre actif.
   Les audits sont inactifs par défaut.

   a. Cliquez sur un audit.

   b. Cochez la case **Actif** pour activer l'audit.

   c. Spécifiez la fréquence d'exécution de l'audit dans le champ **Fréquence** .
   Le centre Séparation en domaines exécute tous les audits marqués avec la même fréquence en même temps. Ne sélectionnez pas **Quotidien** pour les audits qui s'exécutent sur des tables volumineuses.

   d. Répétez les étapes a à c pour chaque audit que vous souhaitez activer.

3. Cliquez sur **Enregistrer**.

Planifier des audits

Spécifiez l'heure et le jour d'exécution des audits.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Vous avez configuré un ou plusieurs audits à exécuter quotidiennement, hebdomadairement ou mensuellement. Le planificateur spécifie les jours et les heures d'exécution de ces audits. Tous les audits avec la même fréquence de planification s'exécutent séquentiellement à partir de l'heure que vous configurez.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Calendriers d'audit**.
   La page Calendrier d'audit s'affiche.
2. Configurez les calendriers d'audit.

   a. Cliquez sur un nom de calendrier.

   b. Spécifiez l'heure de la journée à laquelle exécuter l'audit.
   Les unités de temps utilisent l'horloge de 24 heures (c'est-à-dire que 14 équivaut à 14 heures).

   c. Pour les calendriers hebdomadaires, sélectionnez le jour de la semaine pour exécuter l'audit, où 1 est le dimanche.

   d. Pour les calendriers mensuels, sélectionnez le jour du mois pour exécuter l'audit.

   e. Répétez la procédure pour les autres calendriers.

3. Cliquez sur **Enregistrer** pour enregistrer les changements de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Facultatif :** Cliquez sur **Exécuter maintenant** pour exécuter tous les audits planifiés à la fréquence indiquée en haut du volet droit.
   Par exemple, si le titre du volet est **Calendrier d'audit de domaine : quotidien**, **Exécuter maintenant** exécute immédiatement tous les audits planifiés pour s'exécuter quotidiennement.

Que faire ensuite

Pour afficher l'état d'un audit en cours, dans le Centre Séparation en domaines, cliquez sur le numéro dans la zone **Audits en cours** .

Exécuter immédiatement les audits

Les audits s'exécutent généralement comme prévu. Vous pouvez toutefois exécuter tous les audits sur commande.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas exécuter manuellement des audits individuels. Vous pouvez toutefois exécuter tous les audits configurés avec la même fréquence de planification. Par exemple, vous pouvez exécuter tous les audits configurés pour s'exécuter quotidiennement.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Calendriers d'audit**.
2. Cliquez sur le nom du calendrier d'audit que vous souhaitez exécuter (par exemple, quotidien, hebdomadaire ou mensuel).
3. Cliquez sur **Exécuter maintenant**.

Que faire ensuite

Pour afficher l'état d'un audit en cours, dans le Centre Séparation en domaines, cliquez sur le numéro dans la zone **Audits en cours** .

Afficher les audits avec avertissements et erreurs

Le centre Séparation en domaines fournit des détails sur les erreurs d'audit et les avertissements.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Sur le tableau de bord Centre Séparation en domaines, les **erreurs** et **avertissements fournissent des** informations détaillées sur les audits qui ont rencontré des problèmes. Les journaux associés à Séparation de domaine résident sur votre serveur dans la table syslog_domain. Les erreurs sont des problèmes qui nécessitent une attention immédiate. Les avertissements ne conduisent pas à des échecs mais présentent les meilleures pratiques, par exemple, ne pas rendre le nom de domaine trop long.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur le numéro dans la zone **Erreurs** ou **Avertissements** .
   La page **Erreurs** ou **avertissements** s'affiche.
2. Cliquez sur l'un des audits de la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page affiche des informations détaillées sur les problèmes liés à l'audit que vous avez sélectionné. Les messages dans **Détails des résultats d'audit** font référence aux valeurs de la table syslog_domain sur le serveur pour les audits de table qui ont révélé des erreurs ou des avertissements.

3. Pour afficher les journaux sur le serveur qui fournissent des informations sur les audits d'avertissement ou d'erreur :

   a. Copiez la valeur **de l'ID de détail** dans le panneau de gauche d'un avertissement ou d'une erreur.

   b. Sur l'instance exécutant le centre Séparation en domaines, dans le **navigateur de filtre**, saisissez *`syslog_domain.list`*.
   La page Journal du domaine s'affiche.

   c. Dans le champ de recherche de la colonne **Source** , saisissez `=<Detail-ID >` (aucun espace après le signe égal), par exemple, `=f6a00fd29a85b300a9503a81b9169678`.
   La page Journal de domaine affiche uniquement les journaux associés à l'audit avec l'ID de détail que vous avez spécifié. Chaque ligne de la table spécifie un enregistrement différent dans lequel l'audit a trouvé des problèmes. Notez que le champ **Message** de cette page correspond aux valeurs affichées **dans la colonne** Message du centre de services de domaine. Les informations incluses dans le message correspondent au type d'audit.

4. **Facultatif :** Sélectionnez l'une des options suivantes :
   - **Exécuter à nouveau l'audit** : réexécutez un audit pour voir s'il rencontre toujours un avertissement ou une erreur.
   - **Désactiver l'audit** : désactive un audit.
   - **Copier les détails** : copie les détails de l'audit dans le presse-papiers.

Afficher les résultats en cours et en attente

Vous pouvez afficher les audits en cours et en attente pour afficher leur état.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Les audits actifs s'exécutent périodiquement ou sont mis en file d'attente pour s'exécuter comme prévu. Vous pouvez afficher leur état au fur et à mesure de leur exécution.

Procédure

1. Cliquez sur le numéro dans la zone **Audits en cours** pour afficher les audits en cours d'exécution ou en attente d'exécution.
   La page Audits en cours s'affiche.
2. Cliquez sur un audit en cours d'exécution ou en attente pour afficher des informations à son sujet.

Afficher les audits inactifs

Vous pouvez afficher tous les audits inactifs au même endroit et les activer éventuellement.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

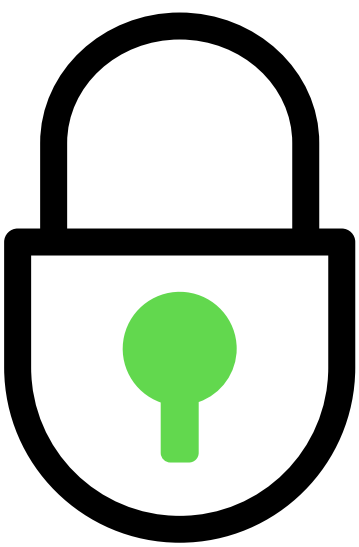
Procédure

1. Cliquez sur le numéro dans la zone **Audits inactifs** .
   La page Audits inactifs affiche tous les audits actuellement désactivés.
2. Cliquez sur l'un des audits pour afficher plus d'informations à son sujet.
3. **Facultatif :** Activez un audit en cliquant sur la case **Actif** et en spécifiant la fréquence d'exécution de l'audit dans le champ **Fréquence** .
4. Cliquez sur **Mettre à jour**.

Authentification

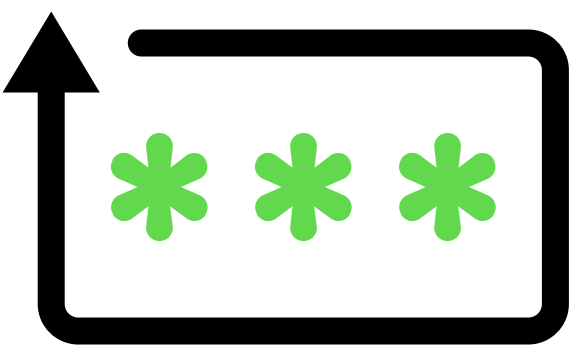
ServiceNow L'authentification de valide l'identité de l'utilisateur qui accède à une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de poste de l'utilisateur.

Premiers pas



Authentification unique (SSO) de plusieurs fournisseurs

Nom d'utilisateur et mot de passe configurés dans les fournisseurs d'identité, qui ont un compte utilisateur correspondant dans la base de données.

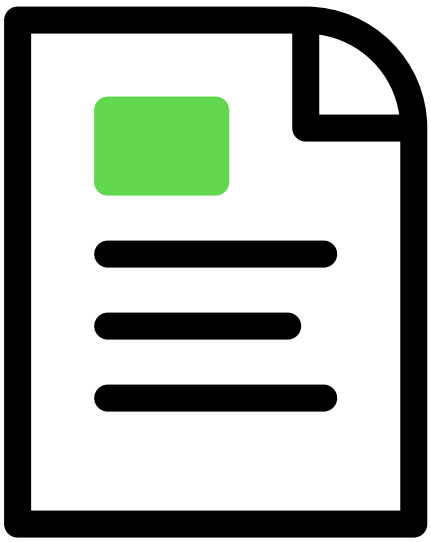


Entrant et sortant OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance sur le système à l'aide d'un protocole d'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



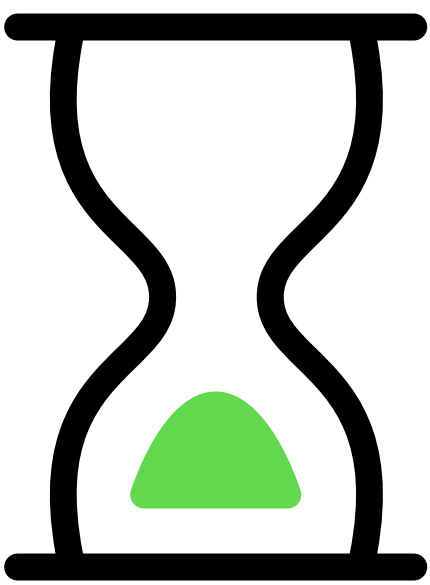
Politique d'accès API

La politique d’accès API définit les autorisations et l’accès à une API qui peuvent être contrôlés par une politique.



Authentification du jeton Digest

Nom d’utilisateur et le secret dans la table, effectuez une opération de hachage spécifique à l’utilisateur, telle que SHA1, SHA 256 ou MD5. Cette valeur doit être ajoutée dans le cadre du suffixe d’URL, qui fonctionne sur le paramètre de requête.



Authentification temporelle limitée

Configurer l’authentification basée sur un lien sur le

ServiceNow

ServiceNow. Le lien configuré peut être partagé avec l’utilisateur par e-mail ou SMS et l’utilisateur peut utiliser ces liens pour se connecter à l’instance.



Authentification multifacteur (MFA)

La MFA vous permet de fournir un deuxième niveau d’authentification qui inclut l’utilisation du code secret d’une application d’authentification, d’une clé matérielle, d’un authentificateur biométrique, d’un SMS ou d’un e-mail.

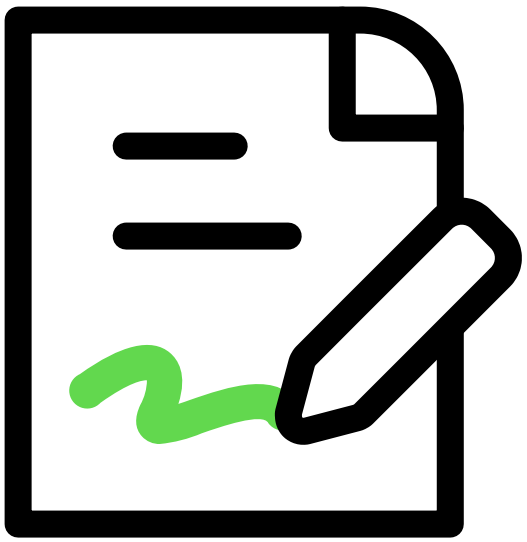
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



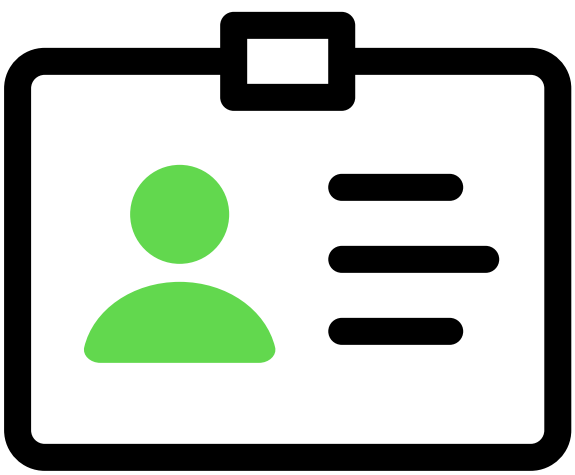
Authentification basée sur certificat

Certificats codés PEM uniques mappés aux utilisateurs au lieu du nom d'utilisateur et du mot de passe pour l'authentification basée sur certificat.



Auto-inscription

Utilisez l'enregistrement automatique des utilisateurs externes pour intégrer un grand nombre d'utilisateurs externes à votre instance.



LDAP

Intégration à un répertoire LDAP (Lightweight Directory Access Protocol) pour rationaliser le processus de connexion de l'utilisateur

Vous pouvez utiliser plusieurs méthodes différentes pour authentifier les utilisateurs. Les informations d'identification de l'utilisateur correspondent à différentes informations d'identification enregistrées pour chaque méthode.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le Okta module d'extension SSO (Authentification unique) est obsolète.
- Pour en savoir plus sur les propriétés de sécurité qui affectent le traitement des autorisations, consultez Contrôle d'accès Paramètres de renforcement de la sécurité de l'instance.
- Vous pouvez utiliser l'authentification SAML et Digest via l'application SSO de plusieurs fournisseurs.

Authentification adaptative

Utilisez le cadre de travail de la politique d'authentification adaptative pour appliquer des contrôles d'authentification contextuelle aux bons utilisateurs au bon moment. L'authentification adaptative utilise des politiques d'authentification pour évaluer les demandes d'authentification, puis refuser ou autoriser l'accès à votre instance en fonction des conditions de politique spécifiées.

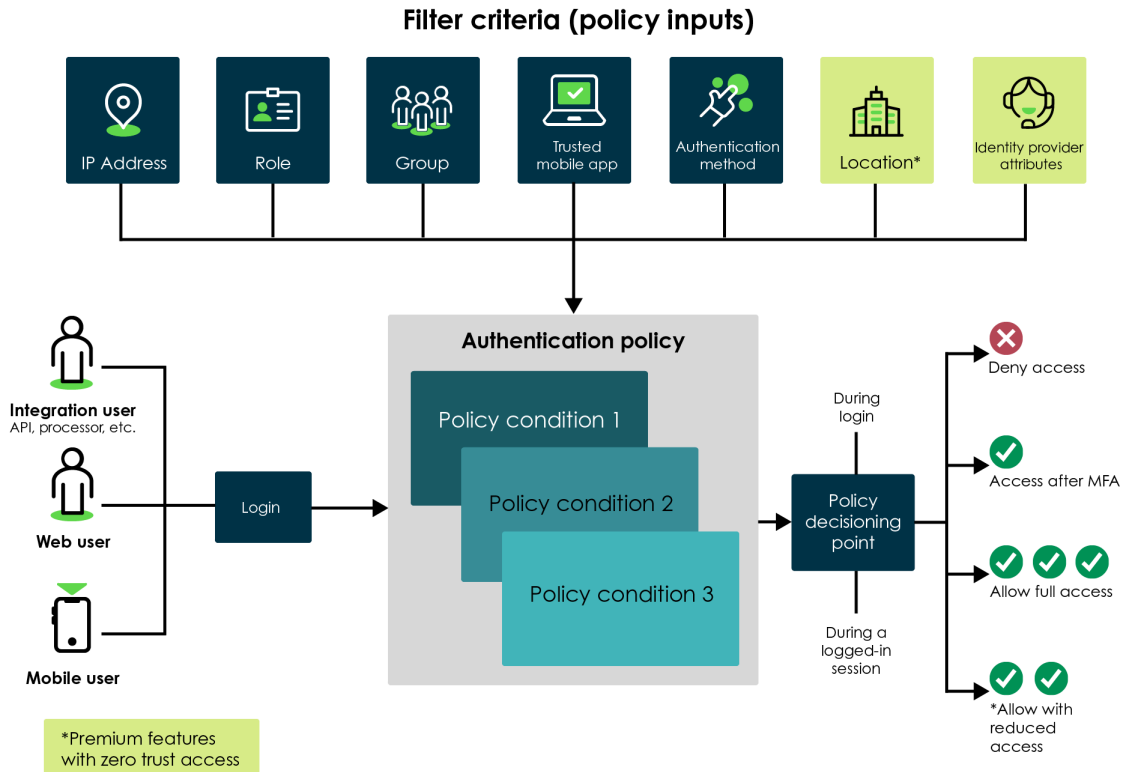
Utilisez des politiques et des contextes d'authentification adaptative pour restreindre l'accès à votre instance pour les utilisateurs et les API en fonction de critères tels que l'adresse IP, le rôle de l'utilisateur et le groupe d'utilisateurs. Vous pouvez configurer les politiques d'authentification intégrées en fonction de vos besoins de sécurité.

Par exemple, un administrateur peut configurer un *`Allow Access Policy`* pour autoriser uniquement les connexions d'utilisateurs situés dans une plage d'adresses IP de confiance et qui sont membres d'un rôle spécifique. Lorsqu'elle est affectée à , *`Post-authentication context`*la politique d'accès refuse l'accès à partir d'adresses IP non approuvées.

Pour définir un message personnalisé dans la langue de votre instance, vous devez ajouter la paire clé/valeur dans `sys_ui_message.list` et mettre à jour l'enregistrement `de` `sys_ui_message` . Lorsque vous vous connectez avec un mot de passe incorrect, le message personnalisé dans la langue préférée s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Composants d'authentification adaptative

Politiques d'authentification

Les politiques d'authentification évaluent les demandes d'authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l'accès en fonction du résultat de l'évaluation des conditions de politique. Par exemple, l'accès n'est autorisé que si toutes les conditions de politique spécifiées dans la **politique d'accès** sont évaluées comme vraies.

Les politiques d'authentification utilisent les informations fournies par les critères de filtre pour les comparer aux conditions de la politique afin de déterminer s'il convient d'accorder l'accès à l'instance. Par exemple, un critère de filtre fournit l'adresse IP d'un utilisateur et une condition de politique détermine si cette adresse se trouve dans la plage spécifique avant d'accorder l'accès. Pour en savoir plus sur les politiques d'authentification, consultez Politiques d'authentification.

Contextes de la politique d'authentification

Les contextes de politique d'authentification définissent comment et quand les politiques sont appliquées pendant le processus de connexion. Le contexte de pré-authentification s'exécute avant que l'écran de connexion ne s'affiche pour l'utilisateur. Le contexte de post-authentification s'exécute une fois que l'utilisateur a entré ses informations d'identification. Pour utiliser une politique, elle doit être affectée à un contexte de politique. Pour plus d'informations sur ces contextes, reportez-vous à la section Contextes de la politique d'authentification.

Critère de filtre

Les critères de filtre (également appelés entrées de politique) sont utilisés comme entrées pour les conditions de politique. Les conditions de politique utilisent ces entrées pour vérifier et répondre aux exigences des demandes d'authentification. Ces entrées fournissent des informations telles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que le rôle de l'utilisateur, la plage IP et le fournisseur d'identité. Pour en savoir plus sur les critères de filtre, reportez-vous à la section Critère de filtre.

Propriétés d'authentification

Utilisez les propriétés d'authentification pour contrôler si l'authentification adaptative est active sur votre instance. Vous pouvez également utiliser des propriétés pour activer le débogage et définir la messagerie que les utilisateurs voient lorsque l'accès est bloqué. Pour plus d'informations sur ces propriétés, reportez-vous à la section Configurer les propriétés d'authentification adaptative.

Politiques d'accès REST API

Vous pouvez utiliser les critères de filtre de l'infrastructure d'authentification adaptative pour restreindre l'accès aux API REST entrantes ServiceNow . Pour plus d'informations, consultez Politiques d'accès REST API.

Séparation de domaine et authentification adaptative

L'authentification adaptative est prise en charge sur les instances séparées par domaine au niveau des conditions de politique d'authentification. Les conditions de politique affectent le domaine dans le champ **Domaine** [sys_domain]. Les conditions de politique dans le domaine global affectent tous les domaines.

Événements d'authentification adaptative

Vous pouvez utiliser la table d'événements d'authentification adaptative pour connaître les événements spécifiques à la fonctionnalité d'authentification adaptative qui se sont produits. Pour plus d'informations, consultez Événements d'authentification adaptative.

Activer l'authentification adaptative

Vous pouvez activer le module d'extension Authentification adaptative (com.snc.adaptive_authentication) pour Authentification adaptative si vous disposez du rôle administrateur.

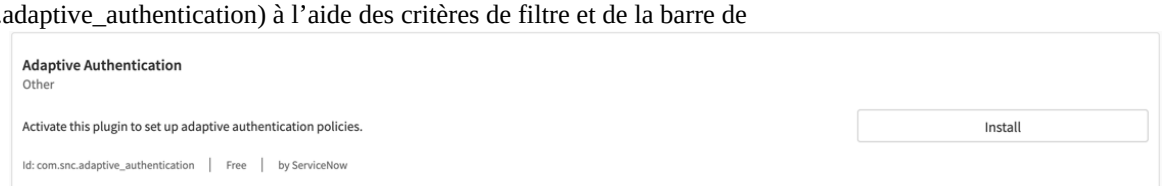
Avant de commencer

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module **d'extension Authentification adaptative** (com.snc.adaptive_authentication) à l'aide des critères de filtre et de la barre de recherche.



Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Que faire ensuite

Configurez vos politiques d'authentification pour appliquer des contrôles d'authentification contextuelle sur votre instance.

Une fois vos politiques configurées. Activez l'authentification adaptative à l'aide de la politique **Activer la politique d'authentification** . Pour plus d'informations sur les propriétés de l'authentification adaptative, reportez-vous à la section Configurer les propriétés d'authentification adaptative.

Critère de filtre

Les critères de filtre (également appelés entrées de politique) sont utilisés comme entrées pour les conditions de politique afin de vérifier et de répondre aux exigences d'une demande d'authentification.

Utiliser des critères de filtre pour fournir des politiques d'authentification d'informations telles que l'adresse IP d'un utilisateur, des rôles ou des groupes. Ajoutez ces critères dans la section Conditions de **politique** de vos politiques.

Il existe sept types de critères de filtre utilisés dans l'authentification adaptative. Vos politiques d'authentification peuvent utiliser un ou plusieurs de ces critères pour évaluer les demandes d'authentification.

Remarque :
Le filtre d'emplacement et le filtre de fournisseur d'identité sont disponibles avec la fonctionnalité d'accès zéro confiance. Pour plus d'informations, consultez Accès zéro confiance (ZTA).

Types de critère de filtre

Type	Description
Critère de filtre d'adresses IP	Utilisez les critères de filtre d'adresses IP pour filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. IPv4 et IPv6 sont tous deux pris en charge.
Critère de filtre de rôle	Utilisez les critères de filtre de rôle pour filtrer les utilisateurs en fonction de leurs rôles.
Critères de filtre de groupe	Utilisez les critères de filtre de groupe pour filtrer les utilisateurs en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.
Critère de filtrage d'emplacement	Utilisez les critères de filtrage d'emplacement pour filtrer les utilisateurs en fonction de leur localisation.
Fournisseur d'identité Critères de filtre d'attribut	Utilisez les attributs du fournisseur d'identité reçus de la réponse SAML de l'IdP comme critère de filtre pour l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critères génériques

En plus des types énumérés précédemment, il existe quatre critères de filtre génériques. Ces critères n'apparaissent pas dans votre navigateur de filtre, mais vous pouvez les sélectionner tout en ajoutant des entrées de politique à vos politiques d'authentification.

Types de critères de filtre génériques

Type	Description
Schéma d'authentification	Utilisez cette option pour filtrer en fonction du schéma d'authentification de l'utilisateur. Ce critère est un type de choix avec deux options : • Nom d'utilisateur et mot de passe, qui désigne une connexion locale • SSO, qui désigne une connexion basée sur plusieurs SSO (SAML, OIDC ou Digest). **Remarque :** Ce critère de filtre est disponible uniquement lorsque le module **d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** [com.snc.integration.sso.multi.installer] est installé.
Fournisseur d'identité	Utilisez cette option pour filtrer en fonction du fournisseur d'identité de l'utilisateur. À utiliser avec les critères du schéma d'authentification pour avoir un contrôle granulaire sur le processus de connexion. Ce critère est une référence à la table **Fournisseurs d'identité** [sso_properties]. **Remarque :** Ce critère de filtre est disponible uniquement lorsque le module **d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** [com.snc.integration.sso.multi.installer] est installé.
MFA basée sur les rôles	Utilisez cette option pour filtrer en fonction de la fonctionnalité MFA basée sur les rôles. Ce critère est un critère de filtre de type booléen qui indique si la MFA basée sur les rôles est activée pour l'utilisateur.
MFA basé sur utilisateur	Utilisez cette option pour filtrer en fonction de la fonctionnalité MFA basée sur l'utilisateur. Ce critère est un critère de filtre de type booléen qui indique si la MFA basée sur l'utilisateur est activée pour l'utilisateur.
Application mobile de confiance	Filtre d'application mobile approuvé pour activer l'accès à l'instance à partir de l'application mobile.

Filtre d'adresses IP

Utilisez les critères de filtre d'adresses IP pour filtrer les utilisateurs en fonction des adresses IP des utilisateurs. IPv4 et IPv6 sont tous deux pris en charge.

Les critères de filtre IP vous permettent de filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une adresse ou à une plage d'adresses spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un critère de filtre d'adresses IP

Les critères de filtre IP vous permettent de filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une adresse ou à une plage d'adresses spécifique.

Avant de commencer

Rôle requis : admin

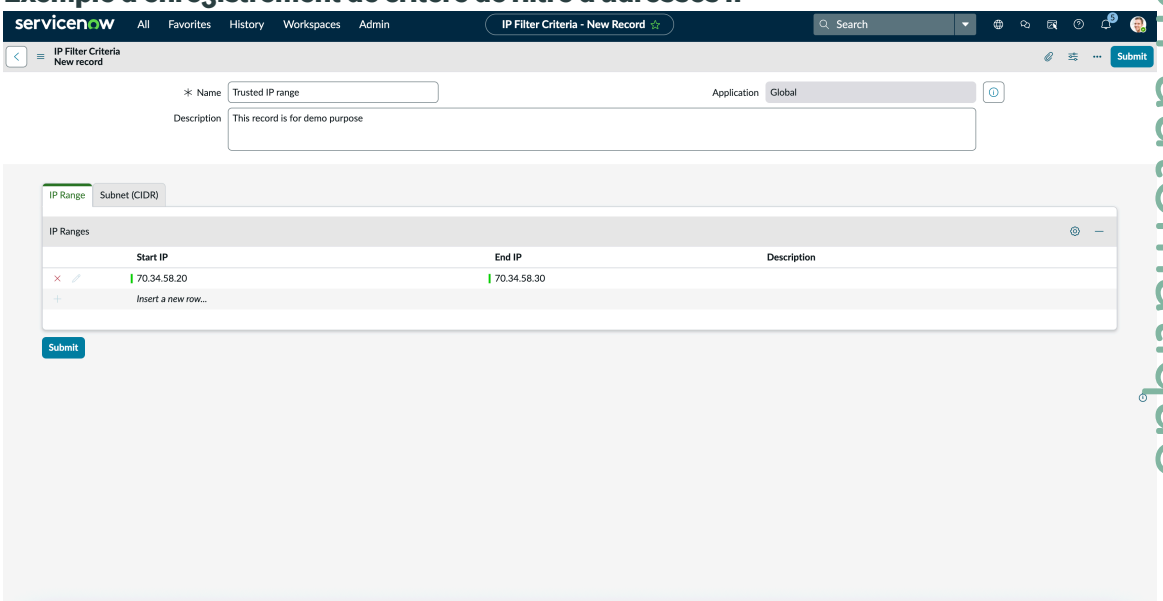
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre d'adresses IP**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtre d'adresses IP

Champ	Description
Nom	Nom permettant d'identifier le réseau IP.
Description	Brève description du réseau IP.
Application	Périmètre de l'application.

Exemple d'enregistrement de critère de filtre d'adresses IP



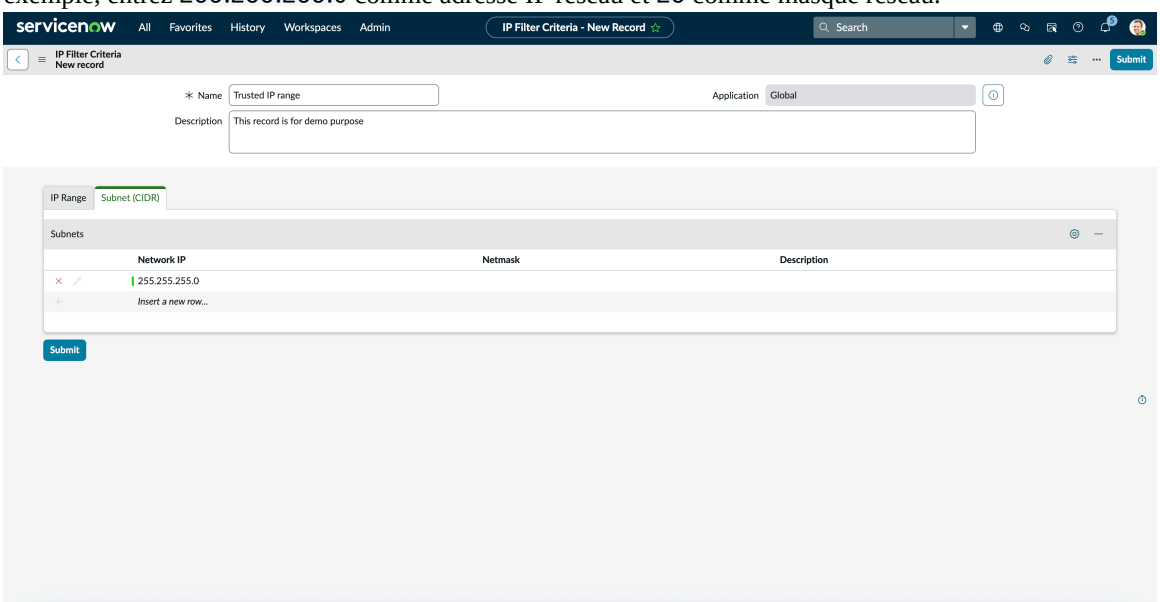
4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
5. Dans l'onglet **Plage IP** , double-cliquez sur **Insérer une nouvelle ligne**.
   Vous pouvez entrer une seule adresse IP ou plusieurs plages d'adresses IP. Par exemple, pour une plage d'adresses IP, entrez `192.0.2.0` dans la colonne **Adresse IP de début** et `192.0.2.255` dans la colonne **Adresse IP de fin** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour une adresse IP unique, veillez à saisir la même adresse IP dans les colonnes Adresse **IP de début** et **Adresse IP de fin** . Lorsque vous entrez une adresse IP dans la colonne **Adresse IP de début** , laissez la colonne **Adresse IP de fin** vide, puis enregistrez l'enregistrement. La colonne **Adresse IP de fin** est automatiquement renseignée avec la même adresse **IP de début** .

6. Dans l'onglet **Sous-réseau (CIDR),** double-cliquez sur **Insérer une nouvelle ligne**.
Entrez l'adresse IP du réseau et le masque réseau au format CIDR (Classless Inter-Domain Routing). Par exemple, entrez 255.255.255.0 comme adresse IP réseau et 25 comme masque réseau.



Filtre de rôle

Utilisez les critères de filtre de rôle pour filtrer les utilisateurs en fonction de leurs rôles.

Les critères de filtre de rôles vous permettent de filtrer les utilisateurs en fonction des rôles. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une liste de rôles d'utilisateur.

Créer un critère de filtre de rôle

Les critères de filtre de rôles vous permettent de filtrer les utilisateurs en fonction des rôles. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une liste de rôles d'utilisateur.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre de rôle**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtre de rôle

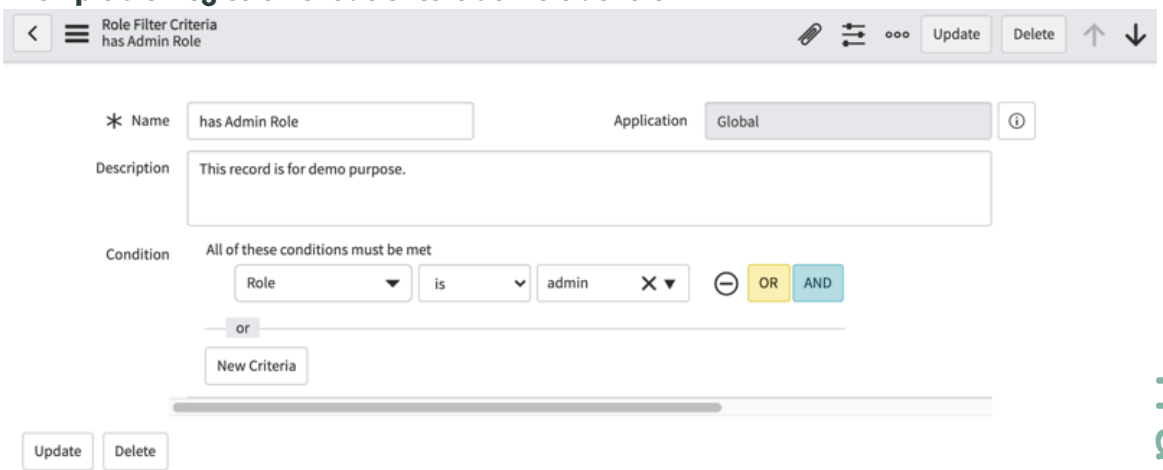
Champ	Description
Nom	Nom permettant d'identifier le rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Périmètre de l'application.
Description	Brève description du rôle.

Exemple d'enregistrement de critère de filtre de rôle



4. Dans **Rôles pour les critères**, double-cliquez sur **Insérer une nouvelle ligne**.
5. Créez une condition pour un rôle spécifique à l'aide du Créateur de conditions.

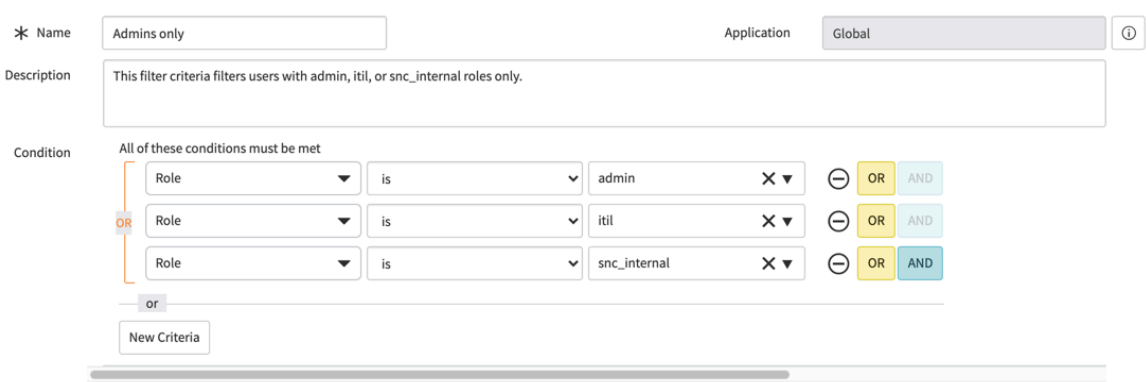
   Par exemple, vous pouvez créer une condition qui autorise uniquement les utilisateurs disposant de rôles administrateur, itil ou snc_internal. Pour plus d'informations sur le générateur de conditions, consultez Créer une instruction de condition à l'aide du générateur de conditions .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Actuellement, la remontée pas à pas n'est pas prise en charge dans les critères de filtre de rôle.
- Les opérateurs suivants ne sont pas pris en charge pour les critères de filtre de rôle :
  - N'est pas
  - Ne contient pas
  - Est différent de
  - Est vide
  - Est identique à
  - N'est pas vide
  - Est une chaîne vide



Filtre de groupe

Utilisez les critères de filtre de groupe pour filtrer les utilisateurs en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.

Les critères de filtre de groupe autorisent ou refusent l'accès de l'utilisateur en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.

Créer des critères de filtre de groupe

Les critères de filtre de groupe autorisent ou refusent l'accès de l'utilisateur en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre de groupe**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

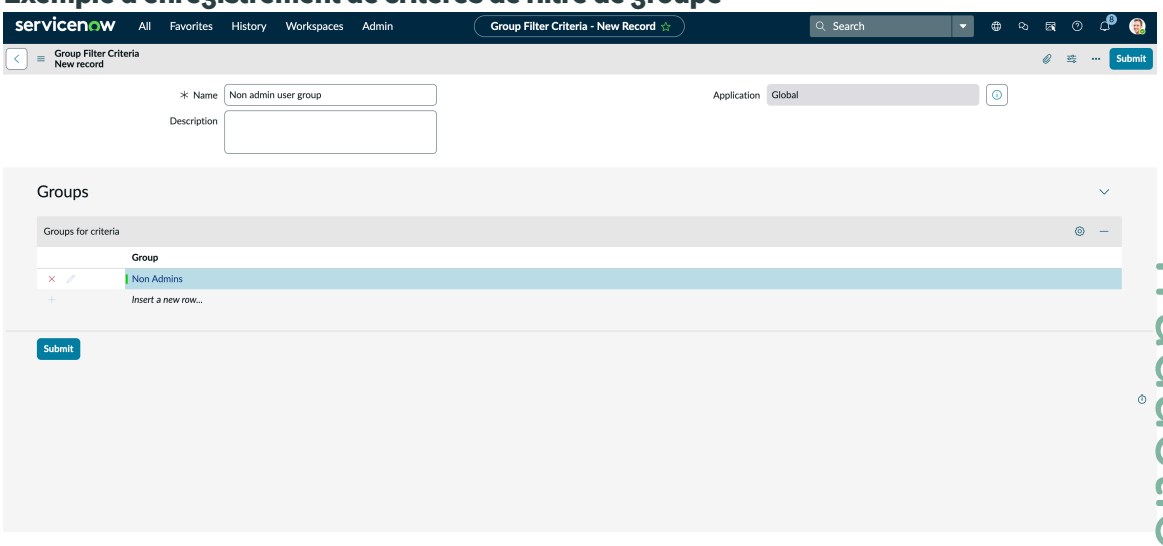
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critère de filtre de groupe

Champ	Description
Nom	Nom identifiant le groupe.
Description	Brève description du groupe.
Application	Périmètre de l'application.

Exemple d'enregistrement de critères de filtre de groupe



4. Dans l'onglet **Grouper pour les critères** , double-cliquez sur **Insérer une nouvelle ligne**.
5. Cliquez sur l'icône , recherchez et sélectionnez un groupe d'utilisateurs.
6. Cliquez sur l'icône d'enregistrement.

Filtre d'emplacement

Les critères de filtrage d'emplacement peuvent être utilisés comme entrée de filtre pour les utilisateurs en fonction de l'emplacement de l'utilisateur.

Le filtre d'emplacement est un critère de filtre que les administrateurs peuvent utiliser lors de l'élaboration des politiques d'authentification en fonction de l'emplacement physique de l'appareil.

Remarque :

- Le filtre d'emplacement est disponible avec la fonctionnalité d'accès zéro confiance. Pour plus d'informations, consultez Accès zéro confiance (ZTA).
- L'instance doit être sur ADCv2. Si l'instance n'est pas sur ADCv2, les informations d'emplacement de l'utilisateur ne seront pas disponibles.

Les critères de filtrage d'emplacement vous permettent d'effectuer les opérations suivantes :

- Agir en tant qu'entrée de politique Agir pour que les conditions de la politique vérifient et répondent aux exigences d'authentification.
- Fournir la possibilité de créer des politiques d'authentification adaptatives en fonction du **pays**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Autorisez ou non l'accès à l'instance à une zone géographique donnée.
- Utilisez la politique de pré-authentification ou de post-authentification basée sur la géolocalisation pour :
  - Empêchez l'accès en provenance de pays sanctionnés, en dehors d'une région étroitement contrôlée par la confidentialité, à la discrétion de l'entreprise.
  - Autorisez l'accès aux zones uniquement à la discrétion de la zone de confidentialité applicable et de l'entreprise.
  - Configurez la liste d'autorisation basée sur le pays pour l'authentification.

Cas d'utilisation

Voici quelques-uns des cas d'utilisation des critères de filtre d'emplacement pour l'authentification adaptative :

- Bloquez l'accès à l'instance à partir d'un pays.
- N'autorisez l'accès à l'instance qu'à partir d'un pays spécifique.
- Appliquez l'authentification renforcée ou la MFA pour vous connecter en fonction du pays.
- Réduire ou limiter les rôles de l'utilisateur en fonction du pays.
- Les critères de filtre d'emplacement peuvent être utilisés pour la MFA, l'accès zéro confiance (ZTA), le contexte de pré-authentification et le contexte de post-authentification.

Identification de l'emplacement

Les services de localisation permettant d'identifier la localisation de l'utilisateur sont fournis par un service tiers - MaxMind.

L'emplacement de l'utilisateur est identifié via le VPN, à partir de l'en-tête x-forwarded-for. Dans le cas où aucun en-tête n'est renseigné par le service, seule l'adresse IP (emplacement) du VPN est affichée comme emplacement de l'utilisateur.

Remarque :
Si des emplacements incorrects sont affichés après la configuration du filtre d'emplacement, consultez l'article de la base de connaissances à résoudre.

Activer l'accès basé sur l'emplacement

Activez **l'option Zéro confiance - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access) pour permettre aux administrateurs de configurer des politiques d'authentification adaptative en fonction de l'emplacement de l'utilisateur.

Avant de commencer
Rôle requis : admin

- Module d'extension dépendant : authentification adaptative
- Type de module d'extension : payant et nécessitant une licence.
- L'instance doit être sur ADCv2. Si l'instance n'est pas sur ADCv2, les informations d'emplacement de l'utilisateur ne seront pas disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Créer un critère de filtrage d'emplacement

Utilisez les critères de filtre d'emplacement pour filtrer les entrées d'authentification des utilisateurs en fonction de l'emplacement de l'utilisateur.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d'authentification adaptative.

Remarque :
Les administrateurs ne peuvent créer la politique en fonction des filtres d'emplacement que si l'emplacement est disponible pour la session utilisateur actuelle.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critères de filtrage de la localisation**.
2. Sélectionnez **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtrage d'emplacement

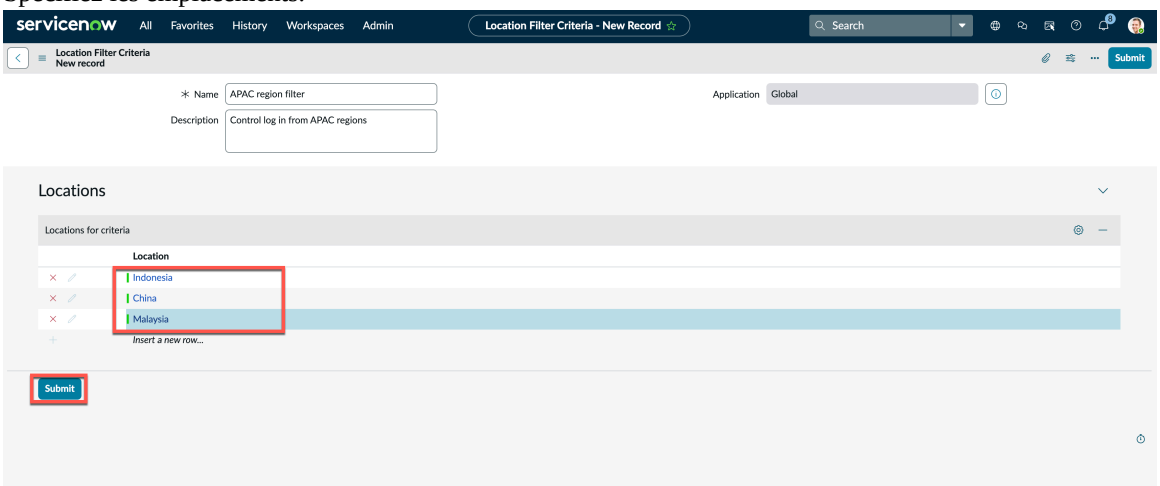
Champ	Description
Nom	Nom permettant d'identifier les critères.
Description	Brève description des critères.
Application	Périmètre de l'application.

4. Dans les sections **Emplacements** , sous l'onglet Emplacements pour les critères, double-cliquez pour **insérer une nouvelle ligne**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Spécifiez les emplacements.



6. Sélectionnez **Soumettre**.

Didacticiel : Utiliser les critères de filtrage d'emplacement

Décrit les étapes à suivre pour utiliser les critères de filtrage d'emplacement dans la politique d'authentification et restreindre l'accès aux utilisateurs en fonction de l'emplacement.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d'authentification adaptative.

Remarque :
Les administrateurs ne peuvent créer la politique en fonction des filtres d'emplacement que si l'emplacement est disponible pour la session utilisateur actuelle.

Dans la procédure suivante, nous vous expliquons comment créer et utiliser les critères de filtre d'emplacement dans une stratégie d'authentification.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Filtre d'emplacement**.
2. Sélectionnez **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom permettant d'identifier les critères.
Description	Brève description des critères.
Application	Périmètre de l'application.

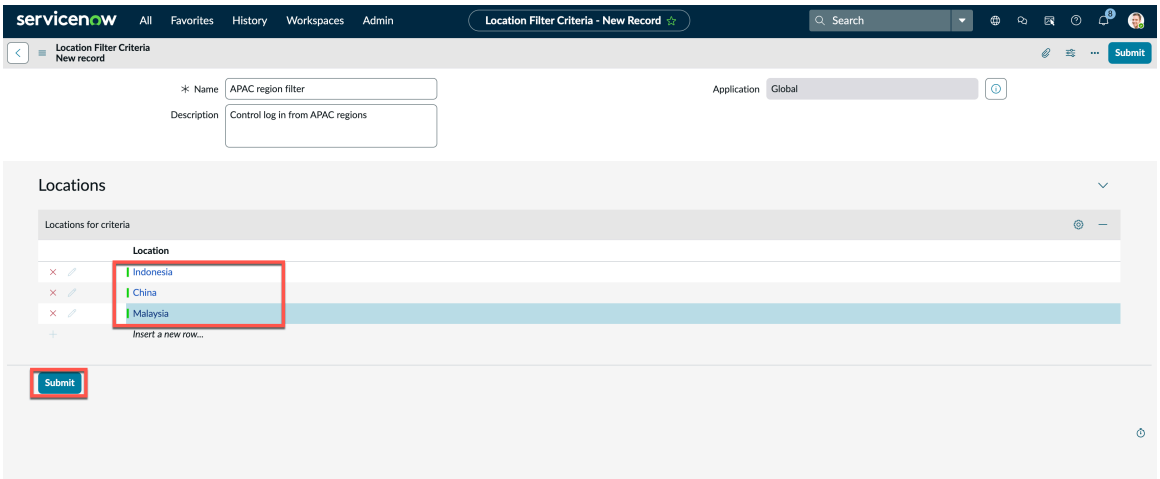
4. Dans les sections **Emplacements** , sous l'onglet Emplacements pour les critères, double-cliquez pour **insérer une nouvelle ligne**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Spécifiez les emplacements.

   Par exemple, utilisez certaines régions APAC pour contrôler les connexions des utilisateurs venant de la région APAC.



   En fonction des critères définis dans l'exemple, vous pouvez contrôler les connexions à partir de l'Indonésie, de la Chine et de la Malaisie pour votre instance.

6. Sélectionnez **Soumettre**.

7. Utilisez les critères de filtre créés dans n'importe quel contexte d'authentification (Pré, Post, MFA) et Accès à la session.

   Pour en savoir plus sur la configuration basée sur le contexte d'authentification et l'accès à la session, consultez :

   - Filtre d'emplacement dans le contexte de pré-authentification
   - Filtre d'emplacement dans le contexte de post-authentification
   - Filtre d'emplacement dans le contexte MFA
   - Filtre d'emplacement pour l'accès à la session

   Vous pouvez utiliser l'ID de propriété - Message d'erreur à afficher à l'utilisateur en cas d'échec de la connexion en raison d'une défaillance de la politique d'authentification (glide.auth.policy.ui.error.message) pour personnaliser le message d'erreur.

Utiliser le filtre d'emplacement dans le contexte de pré-authentification

Utilisez les critères de filtre d'emplacement créés dans le contexte de pré-authentification.

Avant de commencer
Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dont vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtrage d'emplacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

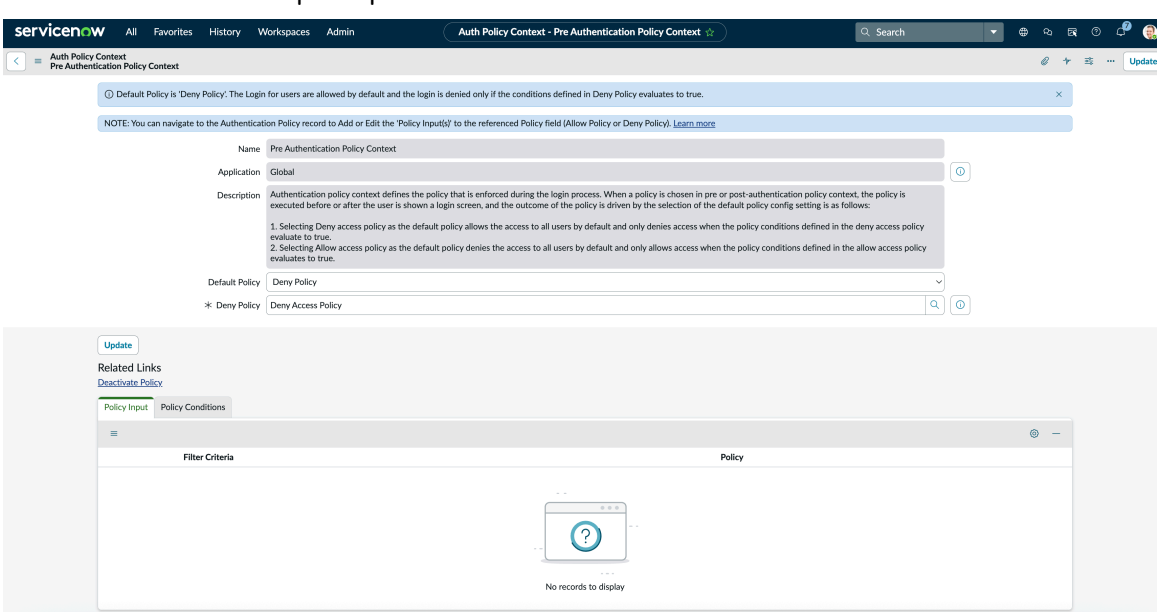
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte de pré-authentification**.

   Lorsqu'une politique est choisie dans le contexte de la politique de pré-authentification :

   - La sélection de la politique Refuser l'accès comme politique par défaut autorise l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions de politique définies dans la politique de refus d'accès sont évaluées comme vraies.
   - La sélection de la politique d'accès comme politique par défaut refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions de politique définies dans la politique d'accès sont évaluées comme vraies.

   L'exemple montre comment vous pouvez restreindre les connexions à partir des emplacements spécifiés. Vous pouvez choisir la politique de refus d'accès et la politique associée (Refuser l'accès) comme politique de pré-authentification et spécifier les entrées et les conditions de la politique.



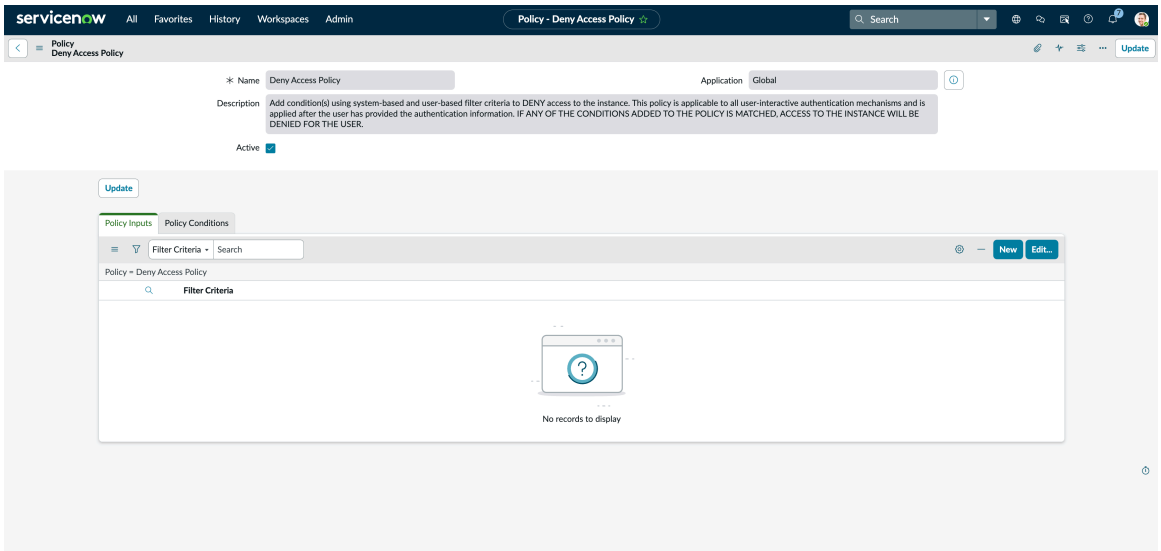
2. Sélectionnez l'icône d'informations, puis **Ouvrir l'enregistrement** pour ouvrir l'enregistrement **Refuser la politique** .

   Remarque :
   L'exemple décrit dans cette tâche est **Refuser la politique**. Vous pouvez également utiliser la **stratégie d'autorisation** et définir les conditions en conséquence pour contrôler les connexions.

3. Dans la section Entrées de politique de refus d'accès, sélectionnez **Nouveau**.

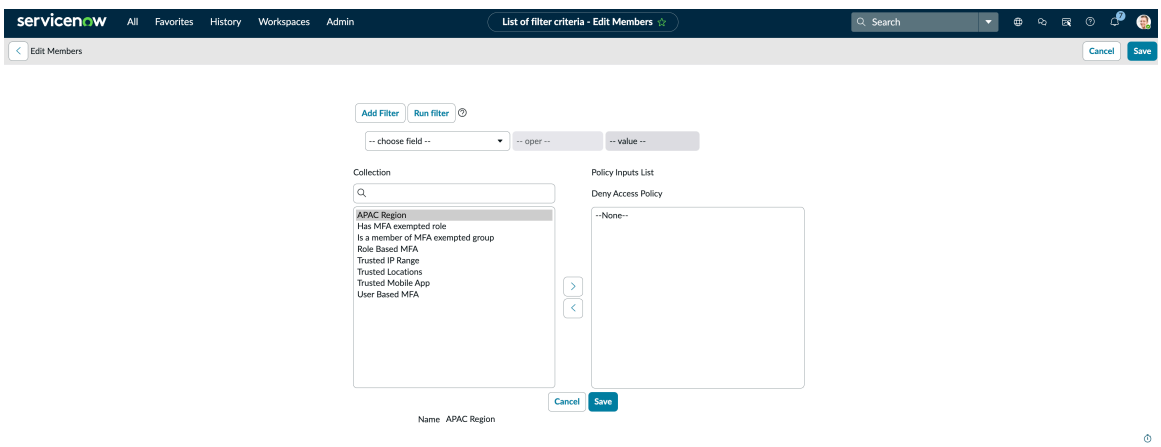
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Ajoutez l’entrée Filtre d’emplacement et **enregistrez**.

   Par exemple, région APAC.

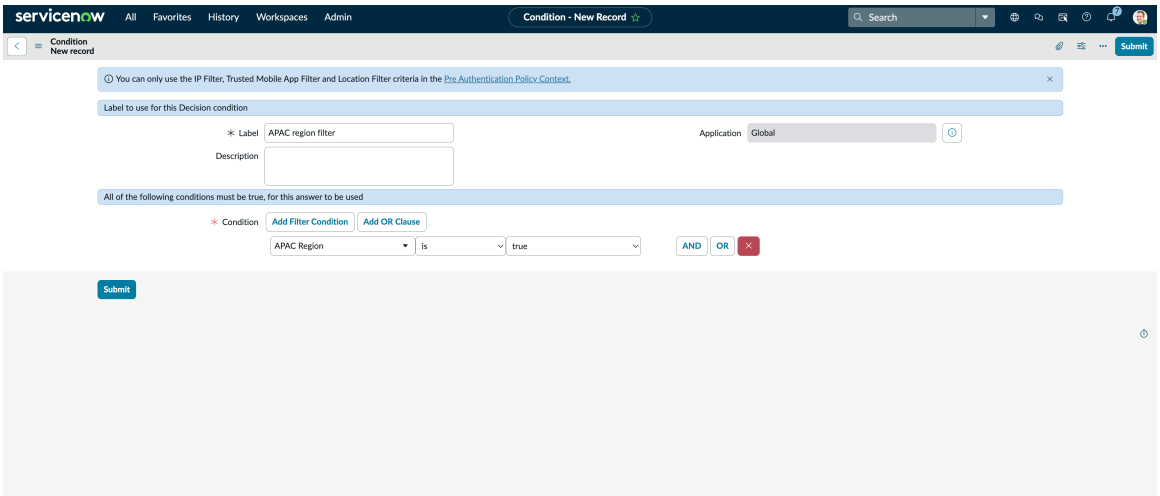


   Le filtre est ajouté en tant **qu’entrées de politique**.

5. Sélectionnez l’onglet Conditions de politique, puis **Nouveau**.
6. Dans la page Conditions, indiquez l’étiquette et les conditions et définissez-les sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Dans cet exemple, la sélection de vrai comme condition implique que l'utilisateur qui se connecte à partir des régions configurées ne pourra pas se connecter à l'instance.
- Si la condition est définie sur faux, seuls les utilisateurs des régions configurées peuvent se connecter à l'instance et les autres utilisateurs ne peuvent pas se connecter à l'instance.

7. Sélectionnez **Soumettre**.
   Les utilisateurs qui sélectionnent le lien d'instance et se connectent à partir des pays configurés verront s'afficher un message d'erreur concernant le refus d'accès (message d'erreur configuré par leurs administrateurs sur la page des propriétés de la politique).

Utiliser le contexte de post-authentification du filtre d'emplacement

Utilisez les critères de filtre d'emplacement créés dans le contexte de post-authentification.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dont vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtrage d'emplacement.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte de post-authentification**.

   Lorsqu'une politique est choisie dans le contexte de la politique de post-authentification :

   - La sélection de la politique Refuser l'accès comme politique par défaut autorise l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions de politique définies dans la politique de refus d'accès sont évaluées comme vraies.
   - La sélection de la politique d'accès comme politique par défaut refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions de politique définies dans la politique d'accès sont évaluées comme vraies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’exemple montre comment configurer des utilisateurs itil avec une condition pour n’accéder à l’instance qu’à partir de l’emplacement spécifié (États-Unis). Et les utilisateurs ITIL ne peuvent pas se connecter depuis d’autres pays.

Une fois que les utilisateurs ont fourni leurs informations d’identification sur la page de connexion. Vous pouvez choisir l’option Autoriser l’accès et la politique associée (Autoriser l’accès) comme politique de post-authentification et spécifier les entrées et les conditions de la politique.

2. Sélectionnez l’icône d’informations, puis **Ouvrir l’enregistrement** pour ouvrir l’enregistrement **Autoriser la politique** .

> **Remarque :**
> L’exemple décrit dans cette tâche est **Autoriser la politique**. Vous pouvez également utiliser la **politique de refus** et définir les conditions en conséquence pour contrôler la connexion.

3. Dans la section Entrées de politique d’autorisation d’accès, sélectionnez **Nouveau**.



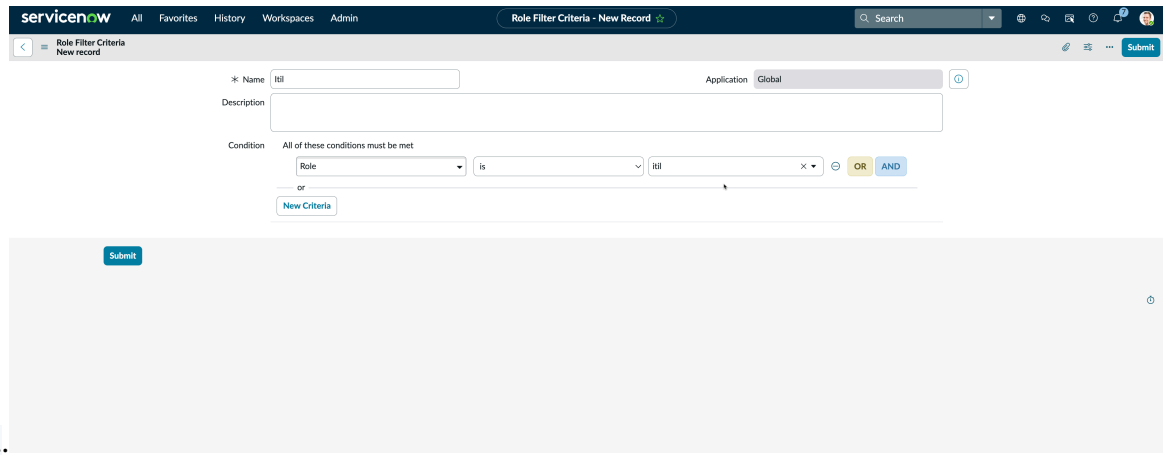
4. Ajoutez les critères de filtre de rôle et les critères de filtre d’emplacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ajout d’un rôle Critère de filtre :

- Créer une entrée de filtre de rôle au format



ITIL.

- Créez une condition de filtre de rôle et définissez-la sur



vrai.

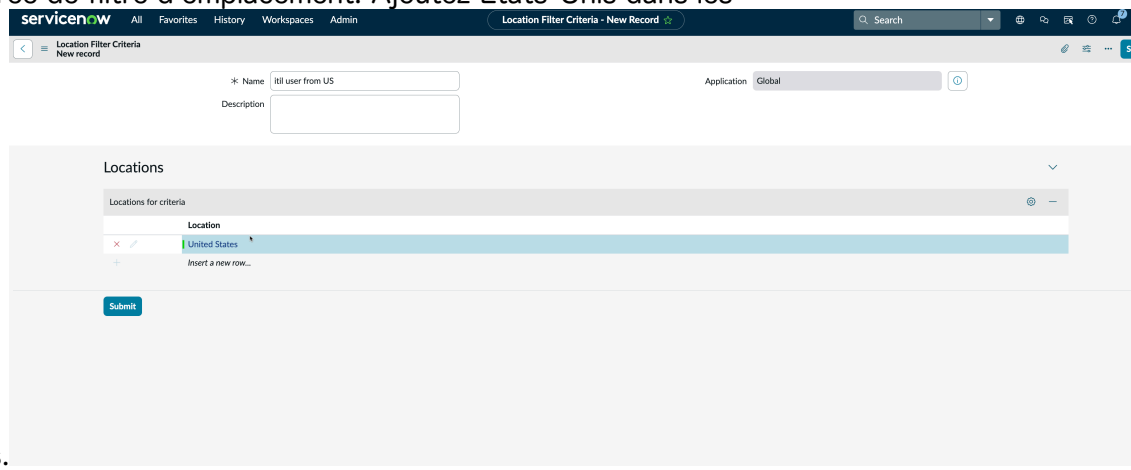
Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à la section Créer un critère de filtre de rôle.

b. Ajout de critères de filtre d’emplacement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créer une entrée de filtre d’emplacement. Ajoutez États-Unis dans les emplacements.



- Créez une condition de filtre d’emplacement et définissez-la sur vrai.



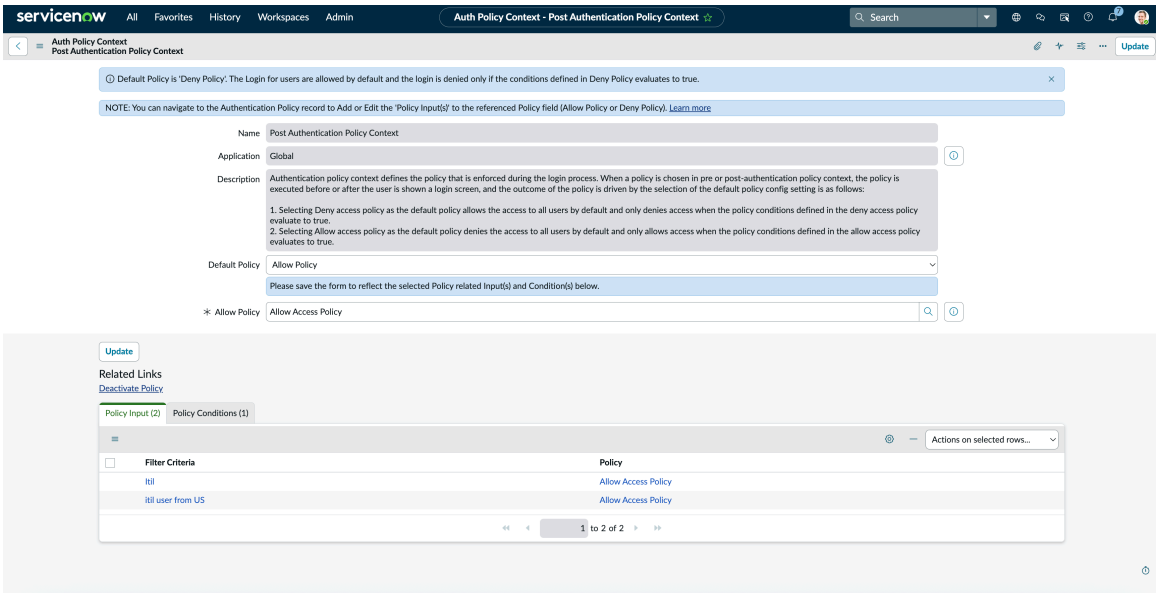
Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à la section Créer un critère de filtrage d’emplacement.

La politique d’autorisation d’accès affiche les entrées et conditions de politique créées lors des étapes précédentes :

- Entrées de politique : itil, utilisateur itil des États-Unis
- Conditions de la politique : connexion de l’utilisateur itil, condition de l’utilisateur itil depuis les États-Unis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Dans cet exemple, la sélection de vrai comme condition implique que les utilisateurs ITIL qui se connectent à partir du pays configuré (États-Unis) peuvent se connecter à l'instance.
- Si la condition est définie sur false, les utilisateurs ITIL du pays configuré (États-Unis) ne pourront pas se connecter à l'instance et les autres utilisateurs ne pourront pas se connecter à l'instance.

5. Sélectionnez **Soumettre** ou **Mettre à jour** pour mettre à jour le contexte de post-authentification.
   Les utilisateurs ITIL qui sélectionnent le lien de l'instance, spécifient leurs informations d'identification, puis se connectent en dehors du pays configuré (États-Unis) affichent un message d'erreur concernant le refus d'accès (message d'erreur configuré par leurs administrateurs sur la page des propriétés de la politique).

Utiliser le filtre d'emplacement dans le contexte MFA

Utilisez les critères de filtre d'emplacement créés dans le contexte MFA.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Dans la procédure suivante, nous vous expliquons comment créer un filtre d'emplacement avec les pays pour lesquels vous souhaitez configurer l'authentification MFA comme second facteur pour l'authentification aux utilisateurs en fonction de l'emplacement.

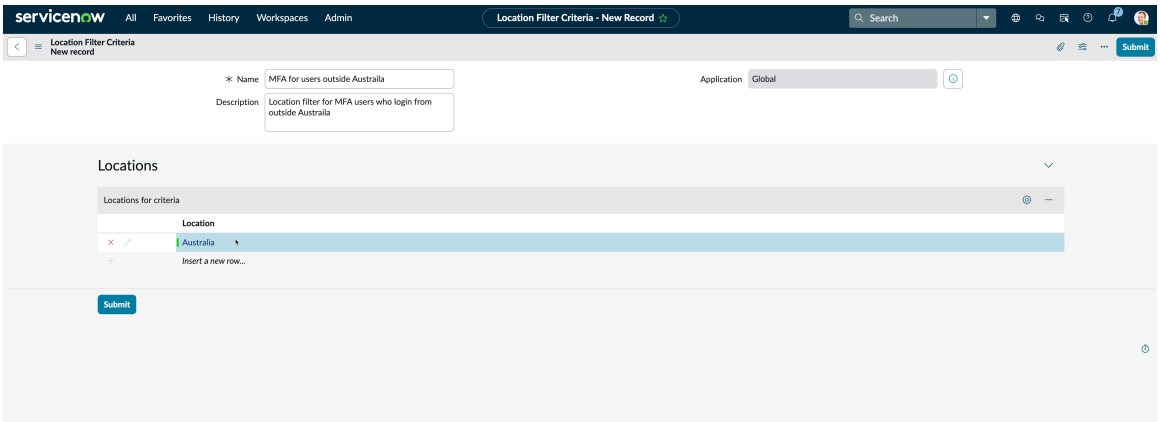
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte MFA**.
2. Sélectionnez l'icône d'informations de **la politique de MFA ascendante** , puis sélectionnez **Ouvrir l'enregistrement** pour ouvrir le **contexte MFA**.
3. Sur la page Politique MFA ascendante, sous l'onglet Entrées de politique, sélectionnez **Nouveau**.
4. Ajoutez l'entrée Filtre d'emplacement et **soumettez**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, vous souhaitez afficher la MFA pour les utilisateurs qui se connectent à l'instance en dehors de l'Australie.



5. Sur la page Politique MFA ascendante, sélectionnez l'onglet Conditions de la politique, puis **Nouveau**.
6. Dans la page Conditions, indiquez l'étiquette et les conditions et définissez-les sur vrai.



7. Sélectionnez **Soumettre**.
8. Sur la page Politique MFA ascendante, activez la politique MFA si elle est **désactivée**.
9. Sélectionnez **Mettre à jour** pour mettre à jour la configuration.

Les utilisateurs en dehors du pays configuré (Australie) qui sélectionnent le lien d'instance, en spécifiant leurs informations d'identification ; s'affiche avec l'écran MFA pour fournir les informations d'identification du deuxième facteur pour se connecter à l'instance.

Utiliser le filtre d'emplacement pour l'accès à la session

Utilisez les critères de filtre d'emplacement créés dans Accès à la session pour réduire les rôles en fonction de l'emplacement de l'utilisateur.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Accès basé sur l'emplacement** (com.snc.zero_trust_location_access).

Dans la procédure suivante, nous vous expliquons comment créer un filtre d'emplacement avec les pays que vous souhaitez supprimer ou limiter les rôles aux utilisateurs en fonction de l'emplacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.
2. Pour créer une configuration de rôle d'accès à la session, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire :

Configuration du rôle d'accès à la session

Champ	Description
Nom	Nom de la configuration
Description	Brève description de la configuration.
Politique	Choisissez la politique d'accès. Utilisez l'icône de recherche pour afficher la liste des politiques. **Remarque :** Vous devez ajouter l'entrée et les conditions du filtre d'emplacement en ouvrant l'enregistrement de politique.
Action	**Supprimez les rôles** ou **limitez-les aux rôles**. ○ **Supprimer les rôles** : lorsque l'utilisateur configuré se connecte, la liste des rôles fournie dans la liste de rôles ou de groupes est supprimée pour la session connectée. ○ **Limiter aux rôles** : lorsque l'utilisateur configuré est connecté, seuls les rôles sélectionnés sont fournis à l'utilisateur et tous les autres rôles sont supprimés pour la session connectée.
Liste de rôles	Choisissez le rôle dans la liste des rôles.
Liste de groupes	Choisissez le rôle dans la liste de groupes.

4. Sélectionner, **soumettre**.

La connexion pour les utilisateurs en fonction des pays configurés est la suivante :

- Si **vous supprimez les rôles**, les utilisateurs des pays configurés dans le filtre d'emplacement seront supprimés avec les rôles configurés pour la session.
- Si **l'option est définie sur Limiter aux rôles**, les utilisateurs des pays configurés dans le filtre d'emplacement n'ont que les rôles configurés pour la session.

Pour en savoir plus sur la suppression ou la limitation des rôles d'une session, reportez-vous à la section Didacticiel : Utiliser l'accès zéro confiance.

Filtre d'attributs du fournisseur d'identité

Utilisez les attributs de fournisseur d'identité reçus de la réponse SAML (Security Assertion Markup Language) et OpenID Connect (OIDC) du fournisseur d'identité (IdP) comme critères de filtre pour l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour extraire tous les attributs d'un IdP via la réponse SAML et OIDC, vous devez effectuer un test de connexion avec l'IdP. Après un test de la connexion réussi, les attributs sont ajoutés dans un nouvel onglet de la page de configuration du fournisseur d'identité.

Pour plus d'informations, consultez les rubriques suivantes :

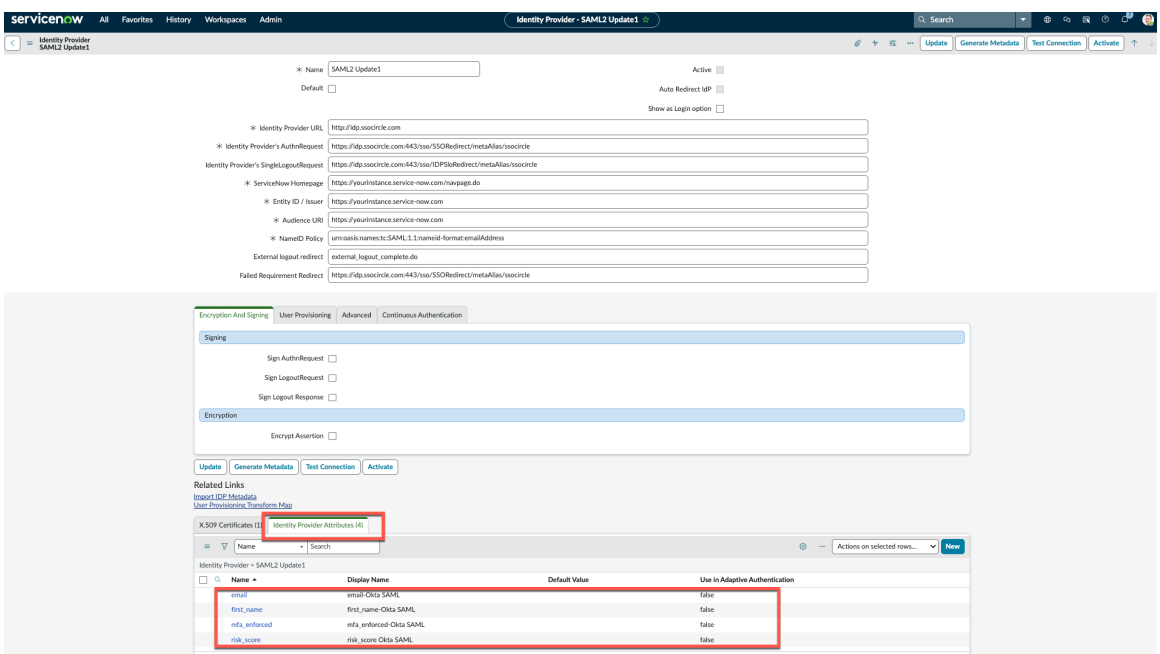
- Attributs du fournisseur d'identité pour le langage de balisage d'assertion de sécurité
- Attributs du fournisseur d'identité pour OpenID Connect

Attributs du fournisseur d'identité pour le langage de balisage d'assertion de sécurité

Utilisez les attributs de fournisseur d'identité reçus de la réponse SAML (Security Assertion Markup Language) et OpenID Connect (OIDC) du fournisseur d'identité (IdP) comme critères de filtre pour l'authentification.

Pour extraire tous les attributs d'un IdP via la réponse SAML, vous devez effectuer un test de connexion avec l'IdP. Après un test de la connexion réussi, les attributs sont ajoutés dans un nouvel onglet de la page de configuration du fournisseur d'identité.

- Le filtre de fournisseur d'identité est disponible avec la fonctionnalité d'accès zéro confiance. Pour plus d'informations, consultez Accès zéro confiance (ZTA).
- Les critères de filtre d'attribut IdP peuvent être utilisés dans Contexte de post-authentification, Accès zéro confiance (ZTA) la relégation de session et Contexte d'authentification multifacteur.



Vous pouvez également ajouter des attributs en sélectionnant **Nouveau** dans la section Attributs du fournisseur d'identité et utiliser ces attributs pour l'authentification adaptative en la définissant sur vrai.

Les **attributs du fournisseur d'identité** sont affichés avec les détails suivants :

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom d'attribut fourni par le fournisseur d'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Critères de filtrage d'emplacement (suite)

Champ	Description
Nom d'affichage	Le nom d'affichage est le nom détaillé utilisé pour les critères de filtre. **Remarque :** Vous pouvez fournir un nom lisible comme nom d'affichage. Dans certains cas, le nom d'affichage fourni par les fournisseurs d'identité est long et illisible.
Valeur par défaut	La valeur par défaut est utilisée pour l'évaluation des critères de filtre si l'attribut est absent de la réponse SAML.
Utiliser dans Authentification adaptative	Option permettant d'utiliser l'attribut dans l'authentification adaptative.

Remarque :
Les attributs renseignés à partir d'Azure IdP ont un nom et un nom d'affichage limités à des caractères, en raison de la longueur du nom de l'attribut.

Vous pouvez également ajouter de nouveaux attributs en sélectionnant **Nouveau** dans la section **Attributs des fournisseurs d'identité** .

Si l'option Utilisation dans l'authentification adaptative est définie sur vrai, l'attribut sélectionné est ajouté en tant que critère de filtre dans les critères de filtre génériques. Par exemple, **risk_score** défini sur vrai. Un nouveau filtre a été créé sur la page Critères de filtre générique.

Utiliser l'attribut du fournisseur d'identité comme critère de filtre pour SAML

Utilisez l'attribut Fournisseur d'identité (IdP) de la réponse SAML (Security Assertion Markup Language) comme critère de filtre pour la politique d'authentification.

Avant de commencer
Rôle requis : admin

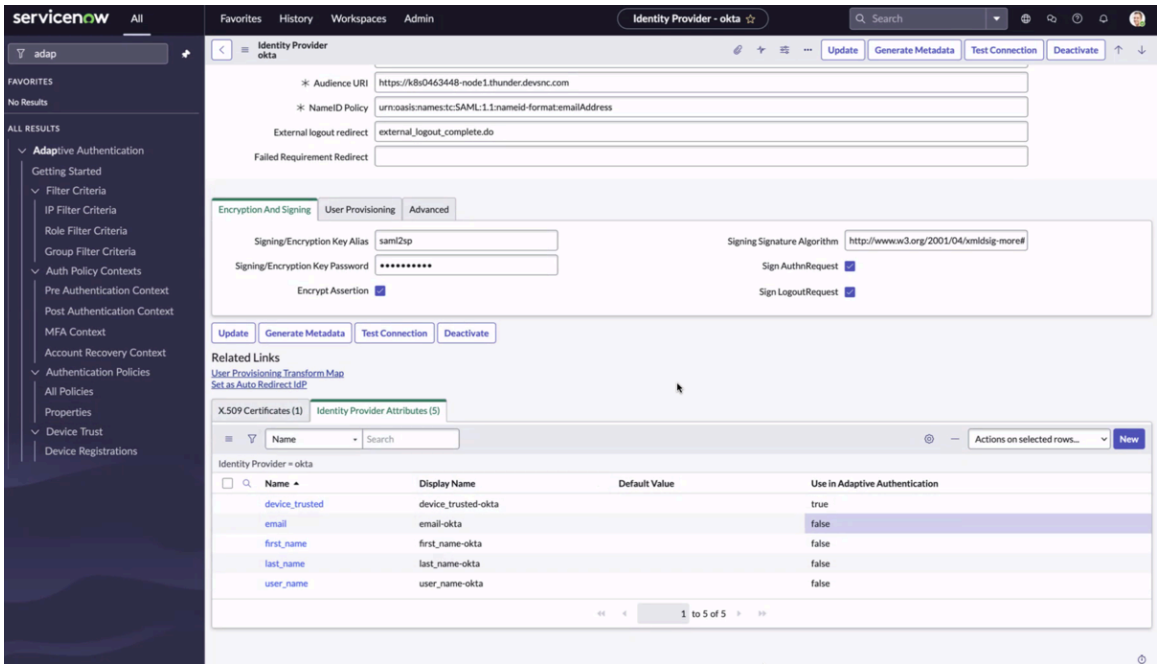
Vous pouvez créer une politique d'accès à la session à l'aide du contexte de la politique (pré-authentification, post-authentification, authentification multifacteur) et des critères de filtre (rôle, groupe, adresse IP, emplacement) avec les entrées et les conditions de la politique.

La procédure suivante montre les étapes de configuration de l'attribut IdP à partir de la réponse SAML en tant qu'entrée de politique pour contrôler l'authentification dans le **contexte de post-authentification**, **l'authentification multifacteur (MFA)** et le **Zero Trust - accès à la session basé sur des politiques**.

Les attributs Okta IdP sont comme illustré dans la capture d'écran suivante. Vous devez définir l'option Utilisation dans l'authentification adaptative sur vrai pour l'utiliser dans le **contexte de post-authentification**, **l'authentification multifacteur (MFA)** et les politiques **d'accès à la session Zero Trust - basées sur** des politiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Les politiques dans la post-autorisation, MFA, Zero Trust - Accès à la session basé sur des politiques s'exécutent une fois que les utilisateurs ont saisi les informations d'identification ou la réponse SSO.

Procédure

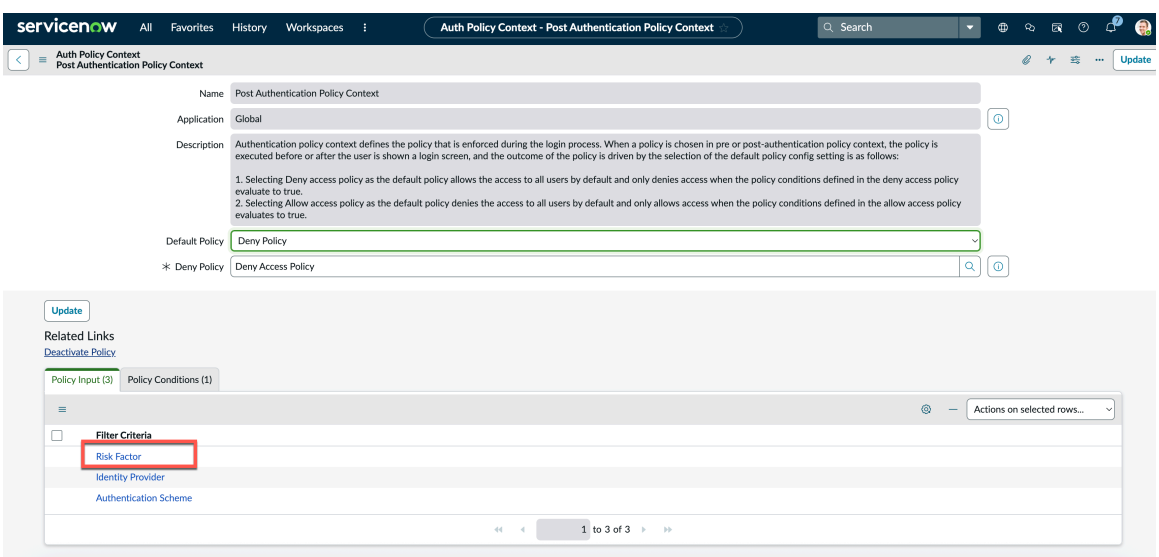
1. Utilisation de l'attribut IdP dans le contexte de la politique de post-authentification.
   Exemple : configuration pour activer les connexions à partir des attributs Okta IdP si l'appareil est approuvé.

   a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de politique de post-authentification.**.

   b. Sélectionnez **Autoriser la politique** et ouvrez l'enregistrement de la politique.

   c. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

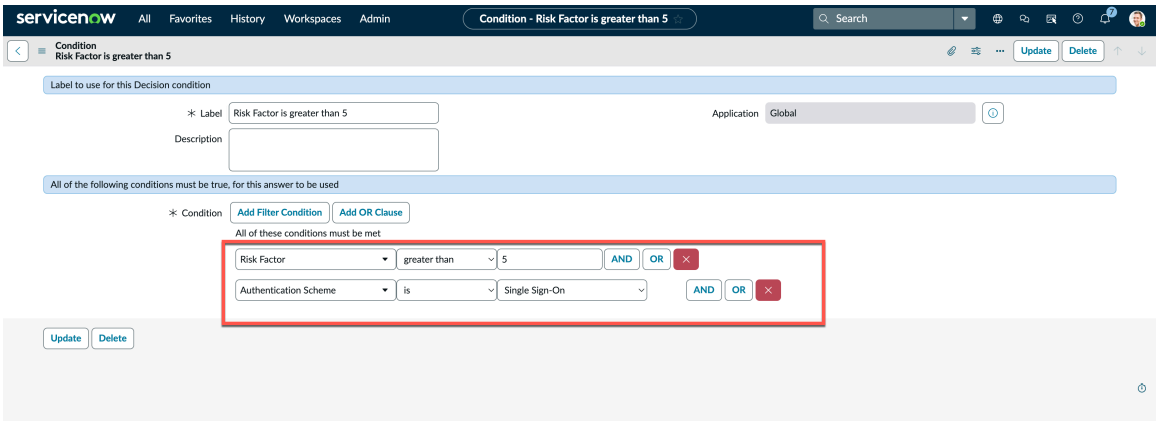
   - **Entrée de politique** : ajouter **device_trusted-okta**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Conditions de politique** : **device_trusted-okta** est approuvé et **le fournisseur d'identité** est okta.



Selon cette configuration, lorsque l'appareil est approuvé par Okta (IdP), l'utilisateur est authentifié auprès de l'instance.

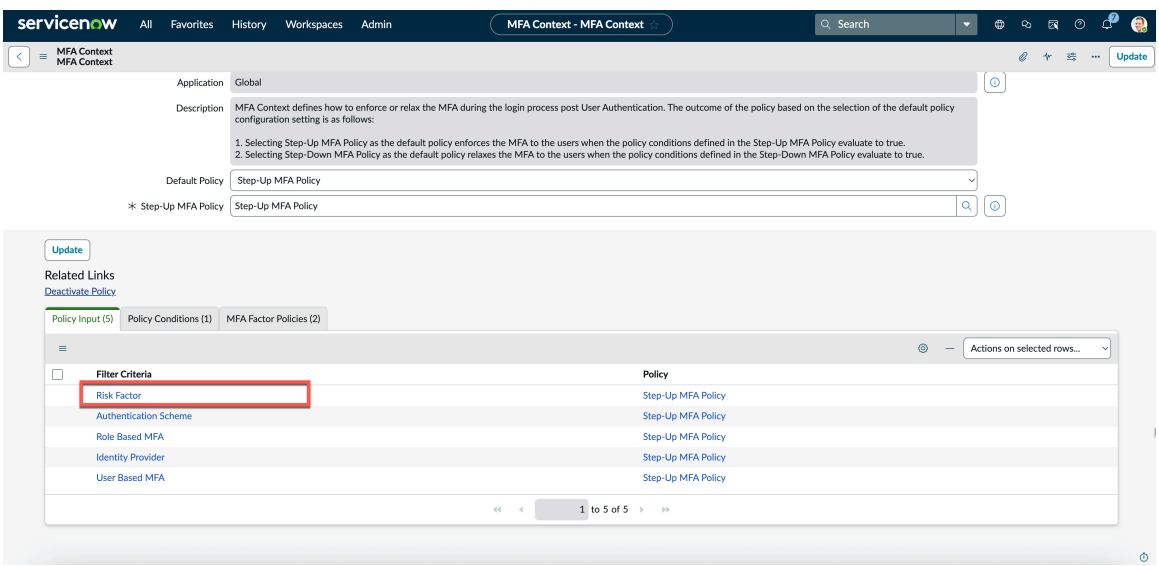
Pour plus d'informations sur la création d'un contexte de post-authentification avec politique et condition, reportez-vous à la section Contexte de post-authentification.

2. Utilisation de l'attribut IdP dans le contexte de la politique de MFA.
Exemple : configuration pour activer la MFA à partir des attributs Okta IdP si l'appareil n'est pas approuvé.

a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique d'authentification MFA.**.

b. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

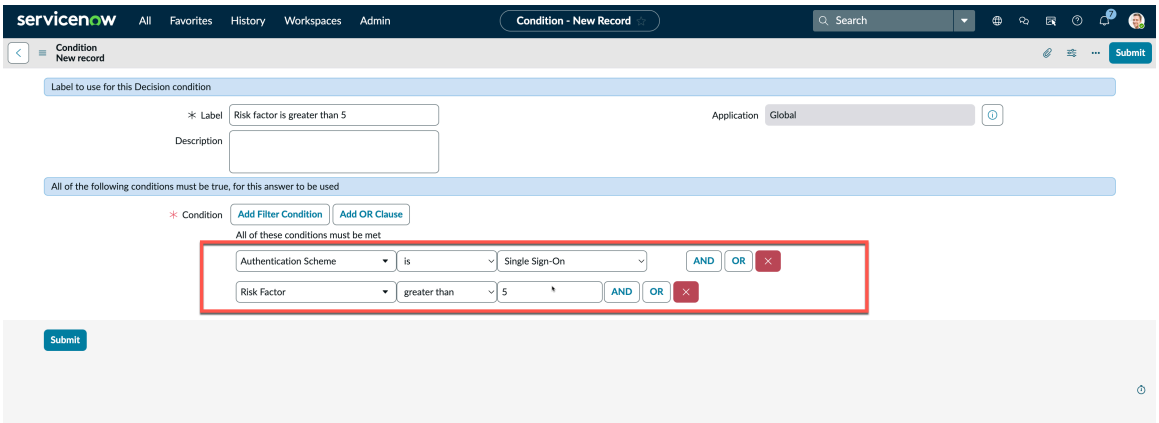
- **Entrée de politique** : ajouter **device_trusted-okta**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Conditions de politique** : **device_trusted-okta** est not_trusted et **Fournisseur d'identité** est okta.



Sur la base de cette configuration, lorsque l'appareil n'est pas approuvé par Okta (IdP), l'utilisateur affiche une authentification à deux facteurs pour se connecter à l'instance.

Pour plus d'informations sur la création d'un contexte MFA avec politique et condition, reportez-vous à la section Contexte d'authentification multifacteur.

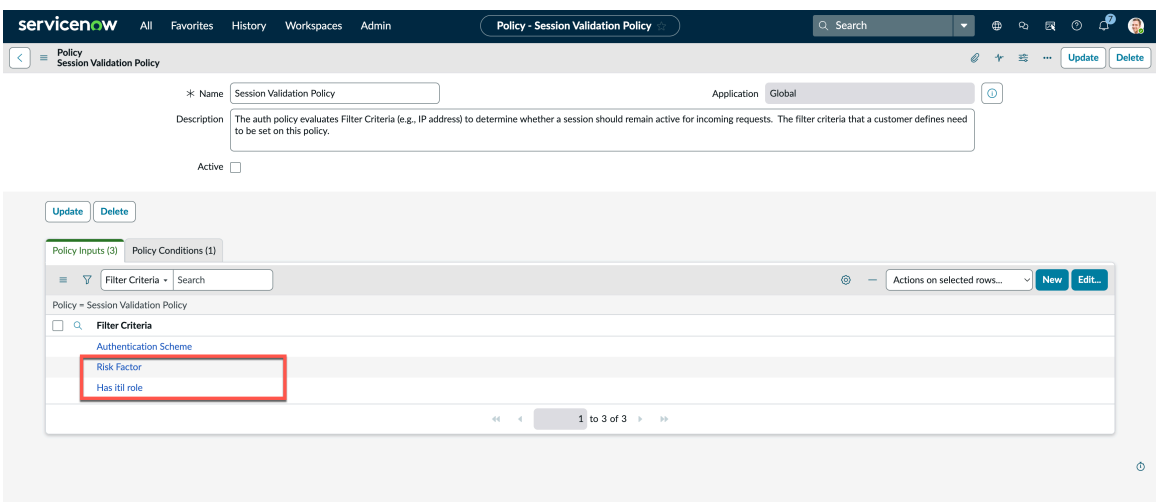
3. Utilisation de l'attribut IdP dans l'accès à la session Zero Trust - basé sur des politiques.
Exemple : configuration pour réduire le privilège du rôle ITIL des attributs Okta IdP si l'appareil n'est pas approuvé.

a. Accédez à la **Tous** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.

b. Créez une configuration du rôle d'accès à la session.

c. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

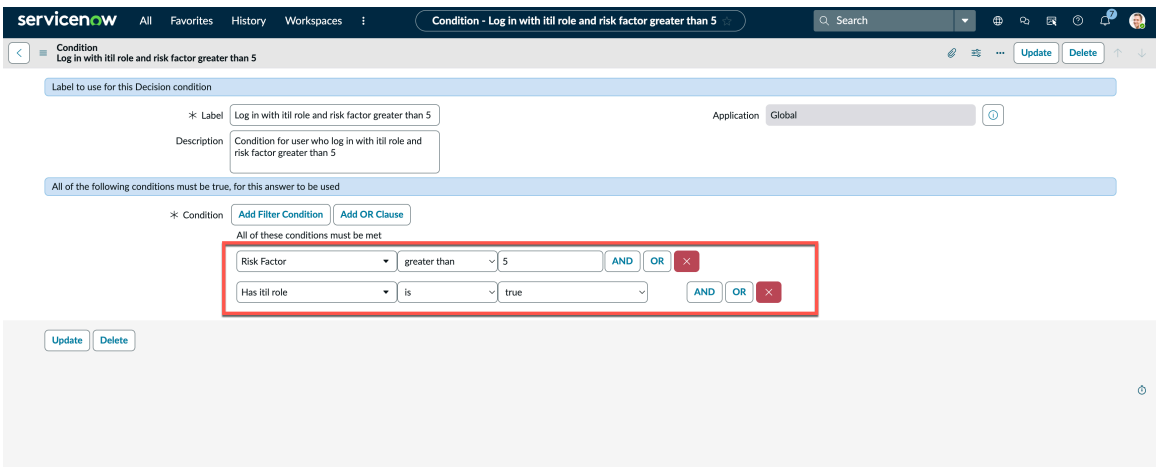
- **Entrée de politique** : Ajouter **device_trusted-okta** et **dispose du rôle itil**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Conditions de politique** : **device_trusted-okta** est not_trusted, **le fournisseur d'identité** est okta et **a le rôle itil** est vrai.



Sur la base de cette configuration, lorsque l'utilisateur itil utilise un appareil qui n'est pas approuvé par Okta (IdP), les privilèges de l'utilisateur sont réduits pour la session connectée.

Pour plus d'informations sur la création d'un accès à la session Zero Trust - basé sur des politiques avec politique et condition, reportez-vous à la section Accès zéro confiance (ZTA).

Attributs du fournisseur d'identité pour OpenID Connect

Utilisez les attributs du fournisseur d'identité reçus d'OpenID Connect (OIDC) du fournisseur d'identité (IdP) comme critère de filtre pour l'authentification.

Vous pouvez créer manuellement les attributs IdP en fonction des réclamations reçues dans le cadre du jeton d'ID.

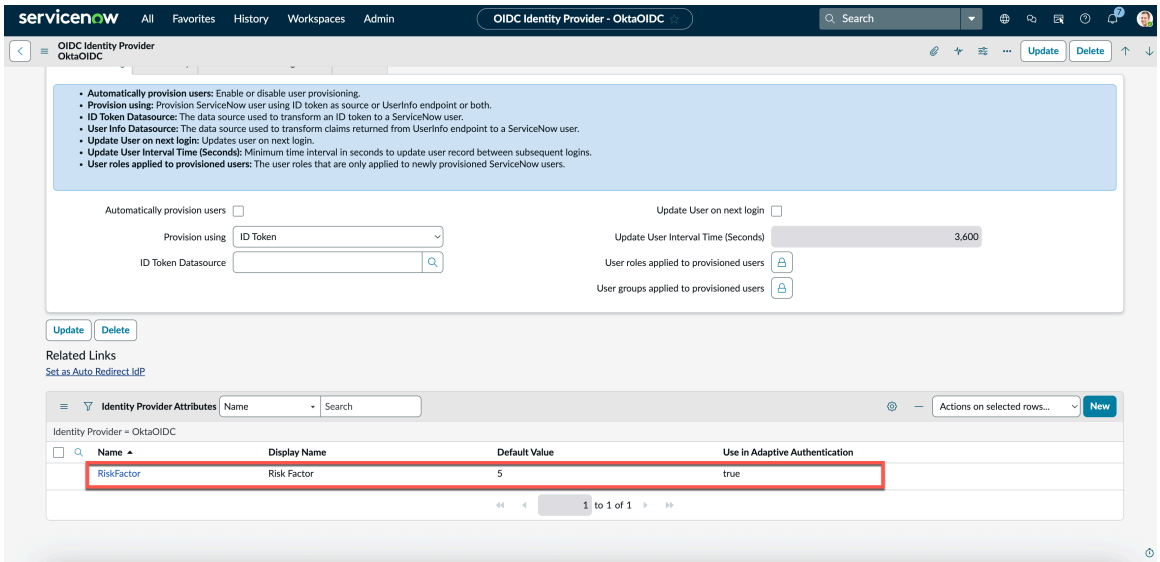
Remarque :

- Le filtre de fournisseur d'identité est disponible avec la fonctionnalité d'accès zéro confiance. Pour plus d'informations, consultez Accès zéro confiance (ZTA).
- Les critères de filtre d'attribut IdP peuvent être utilisés dans Contexte de post-authentification, Accès zéro confiance (ZTA) la relégation de session et Contexte d'authentification multifacteur.

Commencez la configuration en ajoutant des attributs IdP en sélectionnant **Nouveau** dans la section Attributs du fournisseur d'identité, puis utilisez ces attributs pour l'authentification adaptative en la définissant sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le **facteur de risque** défini dans la configuration OIDC dans les attributs du fournisseur d'identité provient des réclamations de jeton d'ID. Cette valeur peut être une réclamation existante ou une réclamation personnalisée telle que configurée du côté IdP. Utilisez cette réclamation dans divers contextes d'authentification pour personnaliser et contrôler le comportement de connexion de l'utilisateur.

Les **attributs du fournisseur d'identité** sont affichés avec les détails suivants :

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom d'attribut fourni par le fournisseur d'identité.
Nom d'affichage	Le nom d'affichage est le nom détaillé utilisé pour les critères de filtre. **Remarque :** Vous pouvez fournir un nom lisible comme nom d'affichage. Dans certains cas, le nom d'affichage fourni par les fournisseurs d'identité est long et illisible.
Valeur par défaut	La valeur par défaut est utilisée pour l'évaluation des critères de filtre si l'attribut est absent de la réponse SAML.
Utiliser dans Authentification adaptative	Option permettant d'utiliser l'attribut dans l'authentification adaptative.

Remarque :
Les attributs renseignés à partir d'Azure IdP ont un nom et un nom d'affichage limités à des caractères, en raison de la longueur du nom de l'attribut.

Vous pouvez également ajouter de nouveaux attributs en sélectionnant **Nouveau** dans la section **Attributs des fournisseurs d'identité** .

Si l'option Utilisation dans l'authentification adaptative est définie sur vrai, l'attribut sélectionné est ajouté en tant que critère de filtre dans les critères de filtre génériques. Par

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

exemple, **risk_score** défini sur vrai. Un nouveau filtre a été créé sur la page Critères de filtre générique.

Utiliser l'attribut du fournisseur d'identité comme critère de filtre pour OIDC

Utilisez l'attribut Fournisseur d'identité (IdP) de la réponse OpenID Connect (OIDC) comme critère de filtre pour la politique d'authentification.

Avant de commencer
Rôle requis : admin

Vous pouvez créer une politique d'accès à la session à l'aide du contexte de la politique (pré-authentification, post-authentification, authentification multifacteur) et des critères de filtre (rôle, groupe, adresse IP, emplacement) avec les entrées et les conditions de la politique.

La procédure suivante montre les étapes de configuration de l'attribut IdP à partir de la réponse SAML en tant qu'entrée de politique pour contrôler l'authentification dans le **contexte de post-authentification**, **l'authentification multifacteur (MFA)** et le **Zero Trust - accès à la session basé sur des politiques**.

Les attributs Okta IdP sont comme illustré dans la capture d'écran suivante. Vous devez définir l'option Utilisation dans l'authentification adaptative sur vrai pour l'utiliser dans le **contexte de post-authentification**, **l'authentification multifacteur (MFA)** et les politiques **d'accès à la session Zero Trust - basées sur** des politiques.

Remarque :
Les politiques dans la post-autorisation, MFA, Zero Trust - Accès à la session basé sur des politiques s'exécutent une fois que les utilisateurs ont saisi les informations d'identification ou la réponse SSO.

Procédure

1. Utilisation de l'attribut IdP dans le contexte de la politique de post-authentification.
   Exemple : configuration pour activer la connexion à partir des attributs Okta IdP si l'appareil est approuvé.

   a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de politique de post-authentification.**.

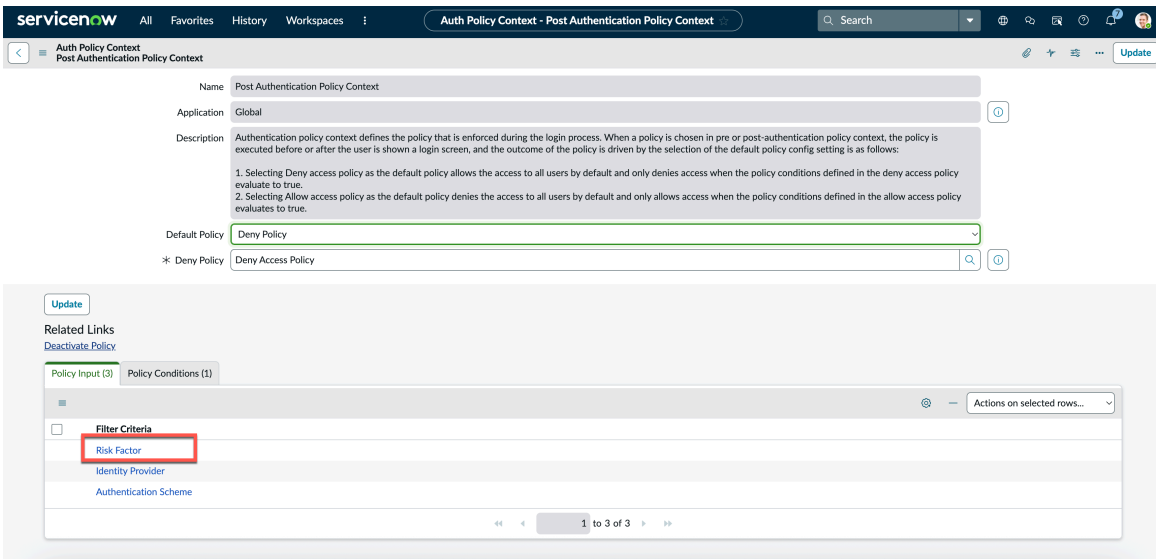
   b. Sélectionnez **Autoriser la politique** et ouvrez l'enregistrement de la politique.

   c. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

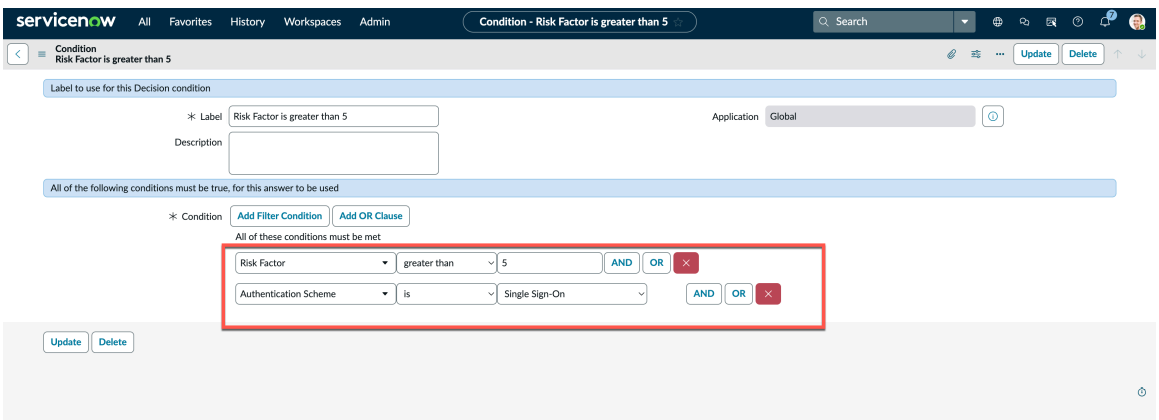
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajouter **un facteur de risque**.



- **Conditions de la politique** : **facteur de risque** supérieur à 5 et **schéma d'authentification** unique sing-on.



Selon cette configuration, lorsque l'appareil est approuvé par Okta (IdP), l'utilisateur est authentifié auprès de l'instance.

Pour plus d'informations sur la création d'un contexte de post-authentification avec politique et condition, reportez-vous à la section Contexte de post-authentification.

2. Utilisation de l'attribut IdP dans le contexte de la politique de MFA.
Exemple : configuration pour activer la MFA à partir des attributs Okta IdP si l'appareil n'est pas approuvé.

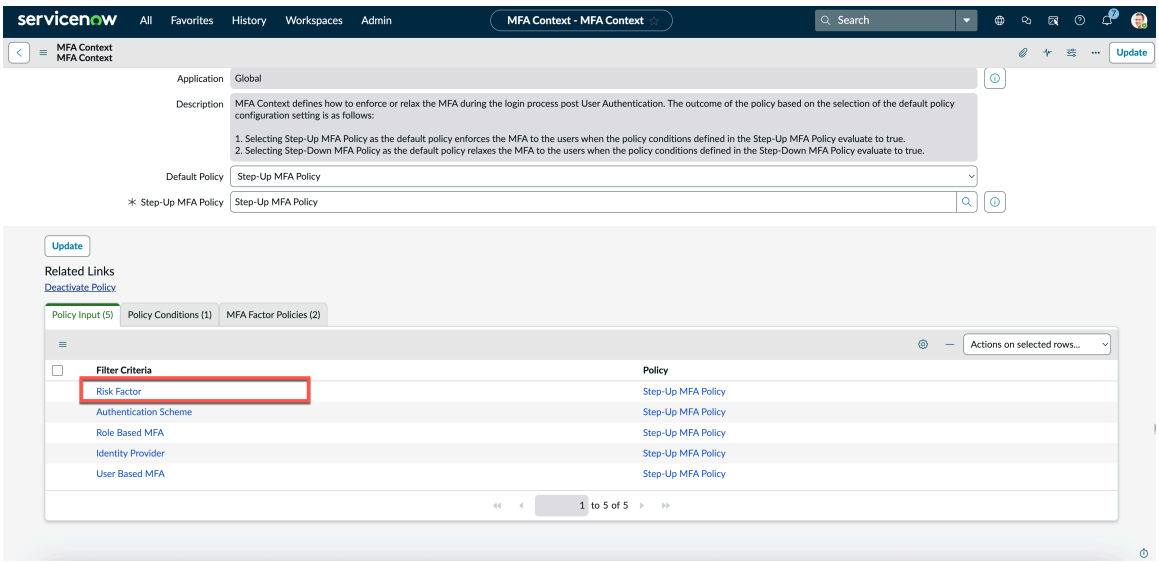
a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique d'authentification MFA.**.

b. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

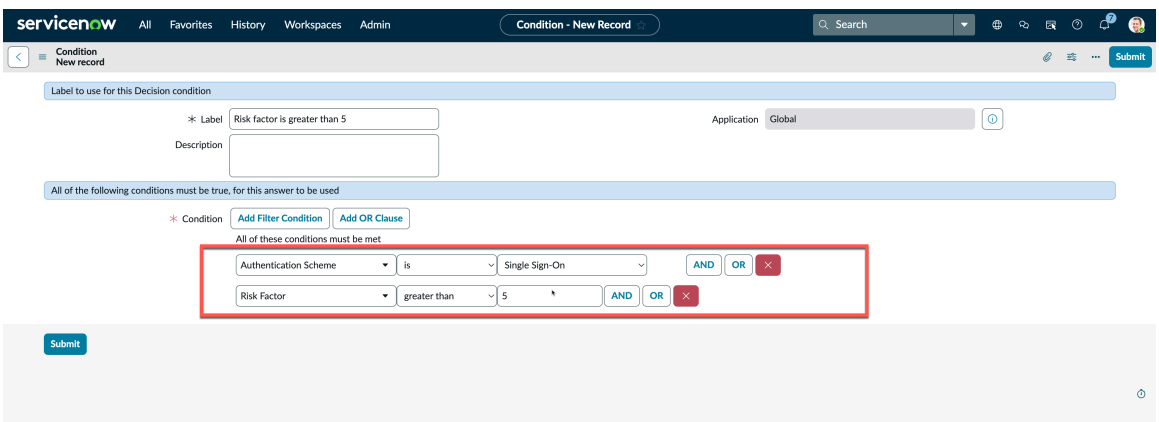
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajouter **un facteur de risque**.



- **Conditions de la politique** : **facteur de risque** supérieur à 5 et **schéma d'authentification** unique sing-on.



Sur la base de cette configuration, lorsque l'appareil n'est pas approuvé par Okta (IdP), l'utilisateur affiche une authentification à deux facteurs pour se connecter à l'instance.

Pour plus d'informations sur la création d'un contexte MFA avec politique et condition, reportez-vous à la section Contexte d'authentification multifacteur.

3. Utilisation de l'attribut IdP dans l'accès à la session Zero Trust - basé sur des politiques.
Exemple : configuration pour réduire le privilège du rôle ITIL des attributs Okta IdP si l'appareil n'est pas approuvé.

a. Accédez à la **Tous** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.

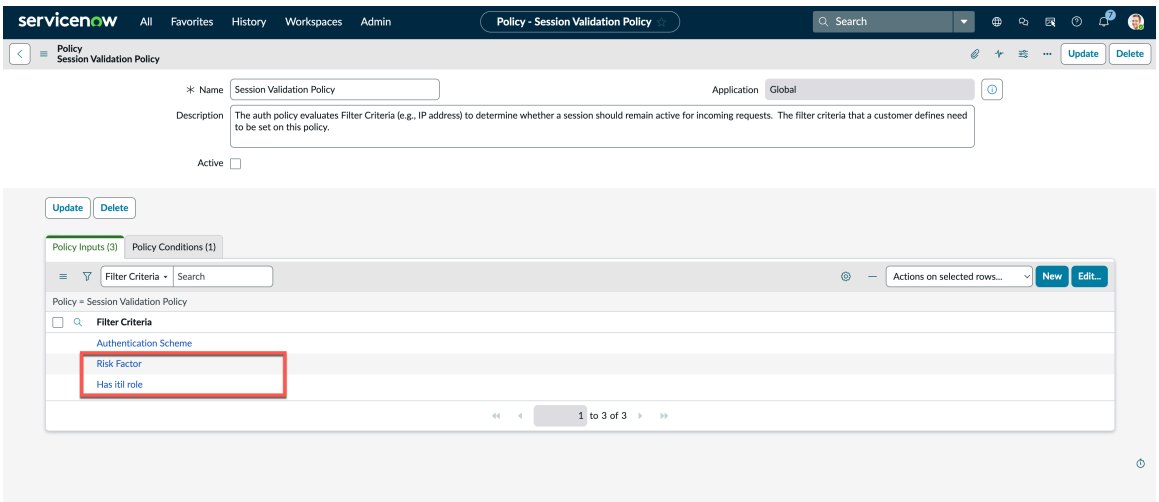
b. Créez une configuration du rôle d'accès à la session.

c. Dans l'entrée Politique, créez l'entrée de politique et la condition de politique.

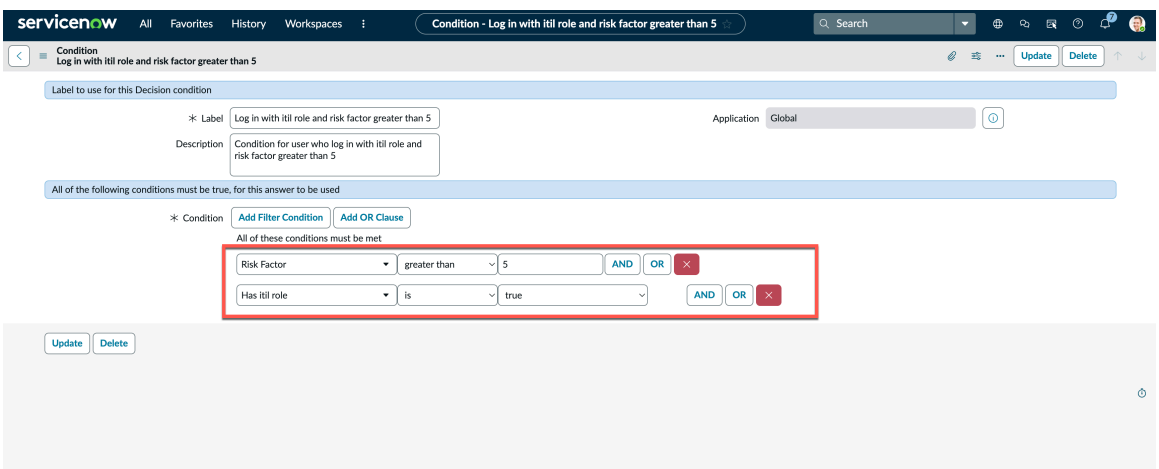
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajoute un **facteur de risque** et **a un rôle itil**.



- **Conditions de la politique** : **facteur de risque** supérieur à 5 et **schéma d'authentification** unique sing-on.



Sur la base de cette configuration, lorsque l'utilisateur itil utilise un appareil qui n'est pas approuvé par Okta (IdP), les privilèges de l'utilisateur sont réduits pour la session connectée.

Pour plus d'informations sur la création d'un accès à la session Zero Trust - basé sur des politiques avec politique et condition, reportez-vous à la section Accès zéro confiance (ZTA).

Contextes de la politique d'authentification

Utilisez les contextes de politique d'authentification pour déterminer comment et quand votre instance applique des politiques d'authentification.

Les contextes d'authentification définissent comment et quand une politique est appliquée pendant le processus de connexion. Affectez une politique à un contexte de politique pour définir les entrées et les conditions concernant la façon dont votre instance gère l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contexte de pré-authentification

Les politiques dans le contexte de pré-autorisation s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'il ne voit un écran de connexion. Vous pouvez utiliser le contexte de pré-autorisation pour autoriser ou refuser l'accès avant que vos utilisateurs ne soient invités à saisir les informations d'identification de connexion en fonction de la politique sélectionnée. Étant donné que ces stratégies s'évaluent avant qu'un utilisateur n'entre des informations, elles ne peuvent pas prendre en compte des critères tels que les rôles ou les groupes d'un utilisateur.

Pour plus d'informations sur ce contexte, reportez-vous à la section Contexte de pré-authentification.

Contexte de post-authentification

Les politiques dans le contexte de post-autorisation s'exécutent une fois que vos utilisateurs ont saisi leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique sélectionnée. Étant donné que vos utilisateurs se sont identifiés via leurs informations d'identification de connexion, la politique peut utiliser les informations utilisateur pour déterminer s'il convient d'accorder l'accès.

Pour plus d'informations sur ce contexte, reportez-vous à la section Contexte de post-authentification.

Contexte MFA (Multi-Factor Authentication)

Les politiques affectées au contexte MFA définissent s'il convient d'appliquer la MFA pendant le processus de connexion. L'application de la MFA par votre instance dépend de la configuration des politiques dans ce contexte. Pour plus d'informations sur ce contexte, reportez-vous à la section Contexte d'authentification multifacteur.

Contexte de récupération du compte

Les administrateurs peuvent configurer la récupération de compte (ACR) pour effectuer des activités de récupération telles que le traitement d'une erreur de configuration SSO ou de certificats expirés. Pour utiliser la récupération de compte, vous devez enregistrer au moins un compte administrateur en tant qu'utilisateur de récupération de compte. L'authentification unique ne peut pas être activée sur votre instance tant qu'au moins un compte n'est pas configuré. Pour plus d'informations sur le contexte qui peut être défini, reportez-vous à la section Contexte de récupération du compte.

Contexte de validation de la session

Le contexte de validation de session peut être utilisé avec le cadre de travail de stratégie d'authentification adaptative. Le cadre de travail utilise des politiques d'authentification pour évaluer les demandes d'authentification (session), puis refuser ou autoriser l'accès en fonction des conditions de la politique. Pour plus d'informations, consultez Contexte de validation de la session.

Politique par défaut

Dans le contexte de la politique, vous pouvez définir une politique par défaut dans le champ **Politique par défaut** . Cette valeur par défaut définit la façon dont votre instance répond au résultat de votre politique. Les options de politique par défaut disponibles sont déterminées par le contexte que vous utilisez. Des détails sur ces options peuvent être trouvés dans les documents décrivant ces contextes individuels.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contexte de pré-authentification

Le contexte de la politique de pré-authentification définit comment et quand une politique est appliquée pendant le processus de connexion. La politique utilisée dans ce contexte s'exécute avant que l'écran de connexion de vos utilisateurs ne s'affiche.

Enregistrement de contexte de pré-authentification

Les politiques dans le contexte de pré-authentification s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'il ne voit un écran de connexion.

Vous pouvez utiliser le contexte de pré-authentification pour autoriser ou refuser l'accès avant que vos utilisateurs ne soient invités à saisir les informations d'identification de connexion en fonction de la politique sélectionnée. Étant donné que ces stratégies s'évaluent avant qu'un utilisateur ne saisisse des informations, elles ne peuvent pas prendre en compte des critères tels que les rôles ou les groupes d'un utilisateur.

Utilisez les champs dans l'enregistrement du **contexte de la politique de pré-authentification** pour définir la façon dont votre instance utilise votre stratégie.

Formulaire de contexte de pré-authentification

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions sélectionnées dans le champ **Autoriser la politique** sont évaluées comme vraies. **Refuser la politique** Autorise l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions sélectionnées par la politique sélectionnée dans le champ **Refuser la politique** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Remarque :

Vous ne pouvez utiliser que les critères Filtre IP, Filtre d'application mobile de confiance et Filtre d'emplacement dans le contexte de la politique de pré-authentification.

Entrées et conditions de la politique

Les onglets **Entrée** de **politique et Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Autoriser** la politique ou Refuser la **politique**. Ces onglets servent de référence, mais ne peuvent pas être utilisés pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

modifier les entrées ou les conditions de la politique. Pour modifier votre politique, accédez à la politique à l'aide de l'icône de référence (icône ⓘ) en regard du champ **Autoriser la politique** ou Refuser la **politique** .

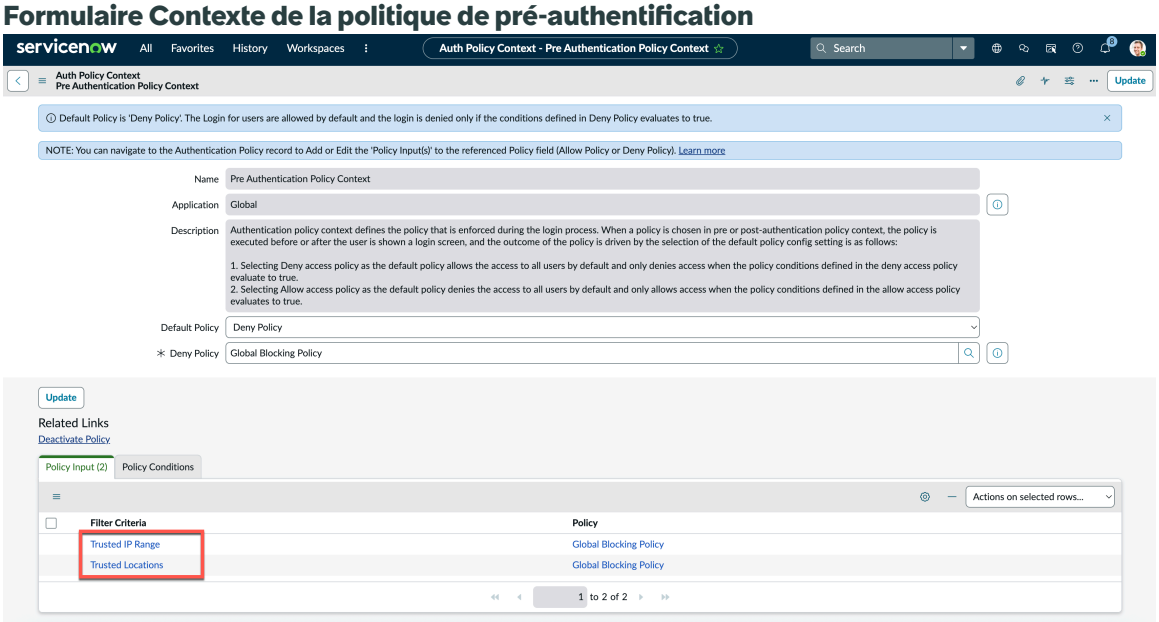
Cet exemple montre un enregistrement de contexte de politique de pré-authentification configuré pour refuser l'accès par défaut. Le contexte utilise une politique appelée **politique de refus d'accès**. Cette politique comporte un ensemble d'entrées et de conditions qui sont affichées dans les onglets **Entrée de politique** et **Condition de politique** .

Remarque :

- Seuls les filtres basés sur l'adresse IP, les filtres basés sur l'emplacement ou le filtre d'application mobile de confiance peuvent être utilisés dans le contexte de la politique de pré-authentification.
- Chaque fois qu'une pré-authentification est définie avec des conditions non absolues ou des critères de filtre, un message d'erreur s'affiche indiquant que la stratégie ou le contexte ne peut pas être configuré. Il est recommandé de valider toutes les entrées pour le contexte de pré-authentification avant de l'exécuter sur l'instance.

  Par exemple : si l'administrateur se trouve en dehors du réseau approuvé et configure un contexte de pré-authentification avec des plages IP, si les plages IP ne correspondent pas à la session en cours de l'administrateur, l'administrateur est bloqué.

Formulaire Contexte de la politique de pré-authentification



Contexte de post-authentification

Le contexte de la politique de post-authentification définit comment et quand une politique est appliquée pendant le processus de connexion. La politique utilisée dans ce contexte s'exécute une fois que l'écran de connexion de vos utilisateurs s'affiche.

Enregistrement de contexte post-authentification

Les politiques dans le contexte de post-autorisation s'exécutent une fois que vos utilisateurs ont saisi leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique sélectionnée. Étant donné que vos utilisateurs se sont identifiés via leurs informations d'identification de connexion, la politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

peut utiliser les informations utilisateur telles que le rôle ou le groupe pour déterminer s'il convient d'accorder l'accès.

Utilisez les champs dans l'enregistrement de contexte de la politique de post-authentification pour définir la façon dont votre instance utilise votre stratégie.

Formulaire de contexte post-authentification

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions sélectionnées dans le champ **Autoriser la politique** sont évaluées comme vraies. **Refuser la politique** Autorise l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions sélectionnées par la politique sélectionnée dans le champ **Refuser la politique** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Entrées et conditions de la politique

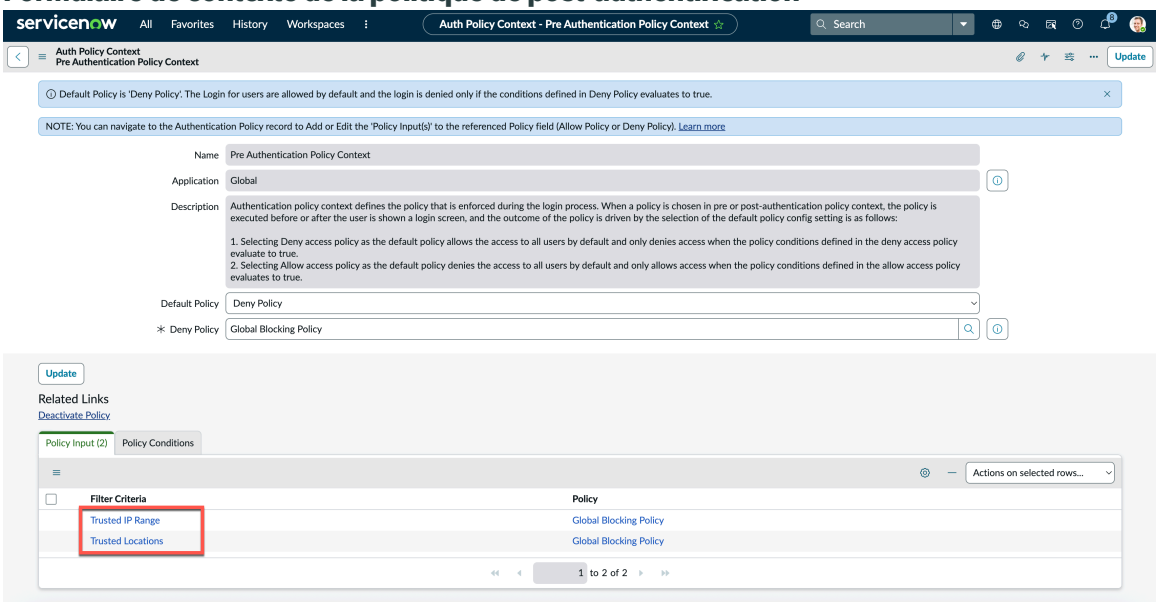
Les onglets **Entrée** de **politique et Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Autoriser** la politique ou Refuser la **politique**. Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône de référence (icône) en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Cet exemple montre un enregistrement de contexte de politique post-authentification configuré pour refuser l'accès par défaut. Le contexte utilise une politique appelée **politique de refus d'accès**. Cette politique comporte un ensemble d'entrées et de conditions qui sont affichées dans les onglets **Entrée de politique** et **Condition de politique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte de la politique de post-authentification



Contexte d'authentification multifacteur

Le contexte politique de l'authentification multifacteur (MFA) utilise une stratégie pour définir comment et quand la MFA est appliquée pendant le processus de connexion.

Enregistrement de contexte MFA

Le contexte de la politique MFA définit si vos utilisateurs doivent fournir une deuxième forme d'authentification lorsqu'ils se connectent. Ce contexte ne refuse pas l'accès à votre instance comme les politiques de post-authentification et de pré-authentification. La politique que vous sélectionnez dans ce contexte a priorité sur les configurations basées sur l'utilisateur ou les rôles pour l'authentification multifacteur.

Pour accéder au contexte MFA, accédez à **Tous** > **Authentification multifacteur** > **Contexte MFA**.

Utilisez les champs dans l'enregistrement de contexte de la politique de post-authentification pour définir la façon dont votre instance utilise votre stratégie.

Remarque :

- Si la politique par défaut est **une politique MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans **la politique MFA** ascendante est évaluée comme vraie. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.
- MFA avec connexion SSO n'est disponible que si la propriété `glide.authenticate.mfa.with.multisso.enabled` est définie sur vrai.
- Vous pouvez accéder à l'enregistrement Politique d'authentification pour ajouter ou modifier les « entrées de la politique » au champ de politique référencé (**Politique de MFA ascendante** ou **Politique de MFA descendante**).
- La politique de contexte MFA s'applique uniquement aux connexions des utilisateurs. Cela ne s'applique pas à l'authentification API, à l'authentification de base et à l'octroi des informations d'identification du mot de passe du propriétaire de ressource OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte MFA

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Politique MFA ascendante** Applique la MFA aux utilisateurs lorsque les conditions de politique définies dans le champ **Politique de MFA ascendante** sont évaluées sur vrai. **Politique MFA descendante** Applique la MFA par défaut. La MFA n'est pas appliquée uniquement lorsque les conditions de politique définies dans le champ **Politique de MFA descendante** sont évaluées comme vraies.
Politique MFA ascendante	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA** ascendante.
Politique MFA descendante	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA descendante**.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Politique de MFA ascendante** ou **Politique de MFA descendante** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône de référence (icône ⓘ) en regard du champ **Politique de MFA ascendante** ou **Politique de MFA descendante** .

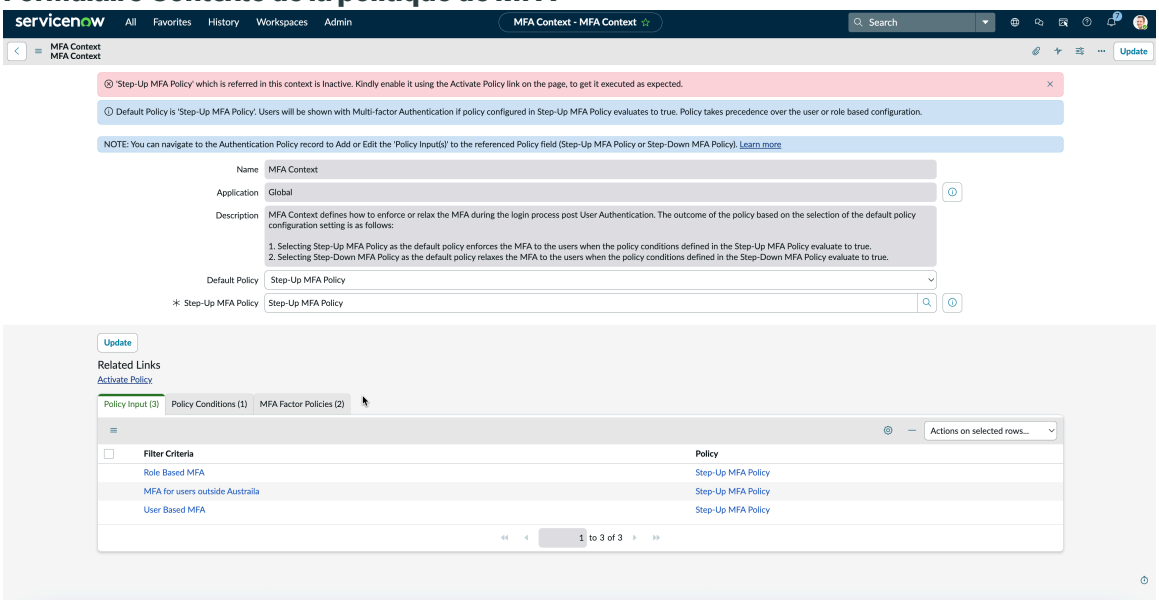
Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais en tant que bonne pratique, il est recommandé d'ajouter de nouvelles conditions de politique à partir de la page de politique.

Cet exemple montre un enregistrement de contexte MFA configuré à l'aide d'une politique MFA ascendante. Cette politique par défaut signifie que la MFA n'est appliquée que lorsque les conditions définies dans la politique sont évaluées comme vraies. Le contexte utilise une politique appelée **politique MFA Step-Up**. Cette politique comporte un ensemble d'entrées et de conditions qui sont affichées dans les onglets **Entrée de politique** et **Condition de politique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Contexte de la politique de MFA



Politiques de facteur MFA

Les politiques de facteur MFA sont un élément essentiel de la posture de sécurité d'une organisation, vous permettant d'appliquer des étapes de vérification supplémentaires au-delà des mots de passe. Ces politiques définissent les méthodes d'authentification auxquelles les utilisateurs doivent accéder, offrant ainsi une approche flexible et personnalisable de l'authentification. Pour plus d'informations, consultez Politiques de facteur d'authentification multifacteur.

Contexte de récupération du compte

Le contexte de récupération du compte utilise une politique pour définir comment et quand la récupération du compte peut être établie.

Les administrateurs peuvent afficher et modifier ce contexte et sa politique associée en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Contexte de récupération de compte**.

Remarque :
Par défaut, la politique est **Autoriser la politique**. La connexion pour les utilisateurs est limitée par défaut et la connexion n'est autorisée que si les conditions définies dans la **politique d'acceptation** retournent la valeur vrai.

Utilisez les champs dans l'enregistrement de contexte de récupération de compte pour définir la manière dont votre instance utilise la politique.

Formulaire de contexte de récupération de compte

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez une option parmi les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

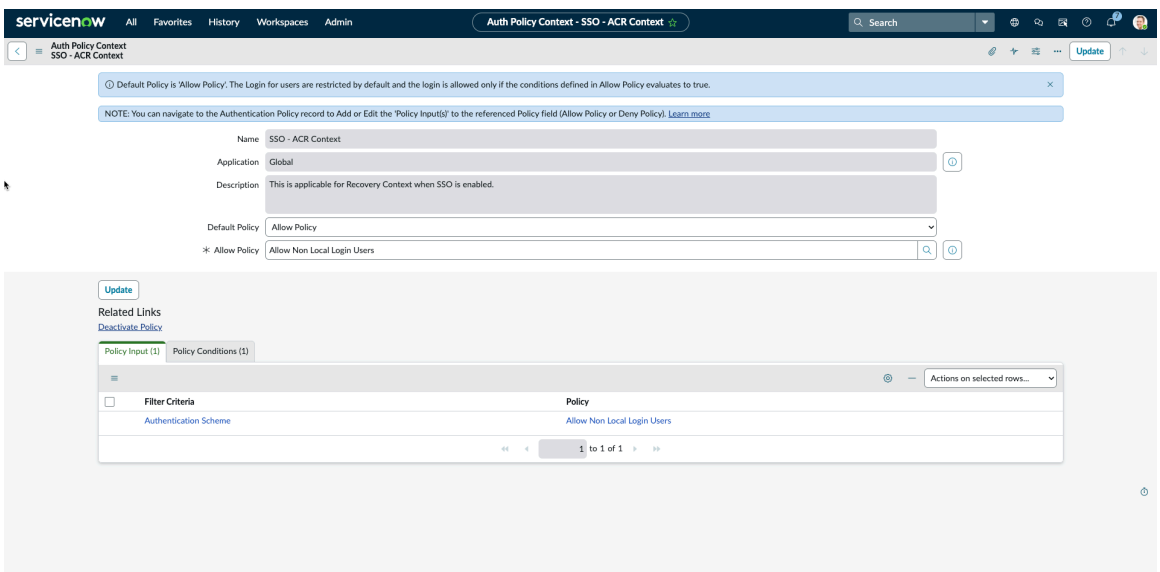
Formulaire de contexte de récupération de compte (suite)

Champ	Description
	• Autoriser la politique • Refuser la politique
Autoriser la politique	Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Entrées et conditions de la politique

Les onglets **Entrée** de **politique et Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Autoriser** la politique ou Refuser la **politique**. Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône d'informations en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais en tant que bonne pratique, il est recommandé d'ajouter de nouvelles conditions de politique à partir de la page de politique.



Contexte de validation de la session

Utilisez le contexte de validation de session comme couche supplémentaire de protection contre le détournement de session ou de cookie.

Vous pouvez utiliser le contexte de validation de session avec le cadre de travail de Authentification adaptative stratégie. Le cadre de travail utilise des politiques d'authentification pour évaluer les demandes d'authentification, puis refuse ou autorise l'accès en fonction des entrées et des conditions de la politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La stratégie de contexte de validation de session peut être utilisée conjointement avec la politique de post-authentification, où un administrateur peut appliquer des restrictions IP à certains ou à tous les utilisateurs pendant la session connectée.

La fonctionnalité Contexte de validation de session évalue les adresses IP en fonction des conditions que vous définissez et autorise l'accès à l'instance au sein d'une session. Les résultats du contexte de validation de session sont les suivants :

- Politique de refus : la sélection de la politique de refus d'accès comme politique par défaut permet aux utilisateurs de continuer la session par défaut. La session se termine uniquement lorsque l'une des conditions de politique définies dans la politique de refus d'accès est évaluée comme vraie.
- Autoriser la politique : la sélection de la politique d'accès comme politique par défaut met immédiatement fin à la session utilisateur, sauf si l'une des conditions de politique définies dans la politique d'accès est évaluée comme vraie.

Remarque :

- Le contexte de validation de session d'une politique d'authentification est défini sur **Autoriser la politique** par défaut.
- Le contexte de validation de session est implémenté via la stratégie Autoriser. Il n'est pas recommandé de définir le contexte sur refuser la politique.

Le contexte de validation de session fonctionne selon le mécanisme suivant :

- Capture l'adresse IP de l'utilisateur lors de la création de session à partir de la demande de l'utilisateur et la stocke dans la session et la base de données.
- Rejette une demande lorsque son adresse IP diffère de celle de la session ou en dehors des plages IP valides définies par le client que vous avez définies.

Remarque :

Le contexte de validation de la session est :

- Disponible uniquement pour les utilisateurs authentifiés.
- Ne s'applique pas aux sessions d'utilisateur invité ni aux applications mobiles natives.
- Facultative et basée sur la condition qu'elle puisse être configurée.
- Exécuté uniquement pour les demandes post-connexion.

Avantages de la validation de session

Le contexte de validation de session présente les avantages suivants :

- Restreint l'accès aux ServiceNow® pirates de l'air qui copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité de la session.
- Restreint l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.
- Configure les différentes règles et plages d'adresses IP par utilisateur, groupe ou rôle pour les connexions utilisateur.

Enregistrement du contexte de validation de session

Les politiques dans le contexte de validation de session exécutent des demandes post-connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez les champs dans l'enregistrement du contexte de la politique de validation de session pour définir la façon dont votre instance utilise votre stratégie.

Formulaire de contexte de validation de session

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte.
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions du champ **Autoriser la politique** sont évaluées sur vrai. **Refuser la politique** Autorise l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions du champ **Politique de refus** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée dans ce contexte. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	La politique utilisée dans ce contexte. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Vous pouvez choisir la **politique de validation de session** en tant que politique d'autorisation ou de refus de politique en fonction de l'entrée et des conditions de la politique.

Remarque :

Vous ne pouvez utiliser que les critères de filtre IP, Rôle et Groupe pour la politique de validation de session.

Entrées et conditions de la politique

Les onglets **Entrée** de **politique et Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Autoriser** la politique ou Refuser la **politique**. Ces onglets servent de référence ; mais elles ne peuvent pas être utilisées pour modifier les entrées ou les conditions de la politique. Pour modifier votre politique, accédez à la politique à l'aide de l'icône de référence (icône ⓘ) en regard du champ **Autoriser la politique** ou Refuser la **politique** .

Activer le contexte de validation de la session

Utilisez le contexte de validation de session pour restreindre l'accès aux pirates de l'air ServiceNow® qui copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité de la session ou restreindre l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

Avant de commencer
Rôle requis : admin

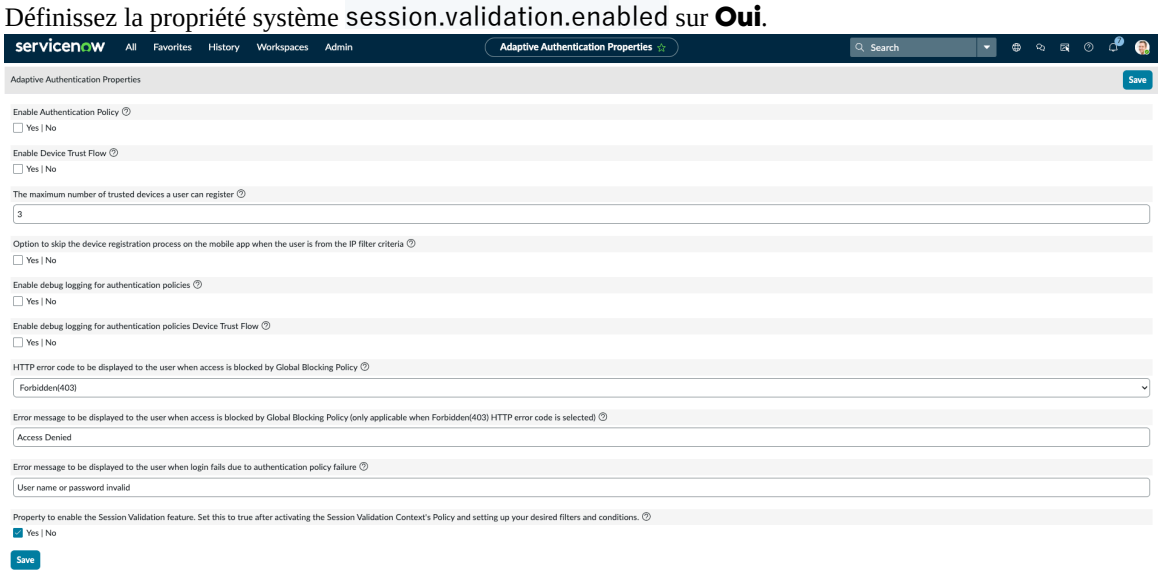
Pour utiliser la validation de session, vous devez procéder comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Sélectionnez la **politique de validation de session** dans la page Politiques (sys_authentication_policy_list.do).
3. Spécifiez les **entrées** et les **conditions de politique**.
4. Définissez les conditions sur **vrai** ou **faux** pour les filtres que vous avez ajoutés.
5. Cochez la case **Actif** pour activer la politique après avoir configuré la validation de session La politique est configurée avec les entrées et les conditions de la politique.
6. Cochez une case **Forcer l'AuthnRequest** pour le fournisseur d'identité par défaut dans la table sso_properties si l'instance a configuré SSO.
7. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
8. Définissez la propriété système session.validation.enabled sur **Oui**.



Résultats

La fonctionnalité de validation de session est activée. Vous pouvez configurer les entrées et les conditions de la politique pour utiliser cette fonctionnalité. Pour en savoir plus, consultez Didacticiel : Configuration de la validation de session.

Didacticiel : Configuration de la validation de session

Configurez la validation de session dans le cadre de travail de l'authentification adaptative pour fournir une couche supplémentaire de protection contre le détournement de session ou de cookie.

Avant de commencer

Rôle requis : admin

Module **d'extension requis : Authentification adaptative** (com.snc.adaptive_authentication)

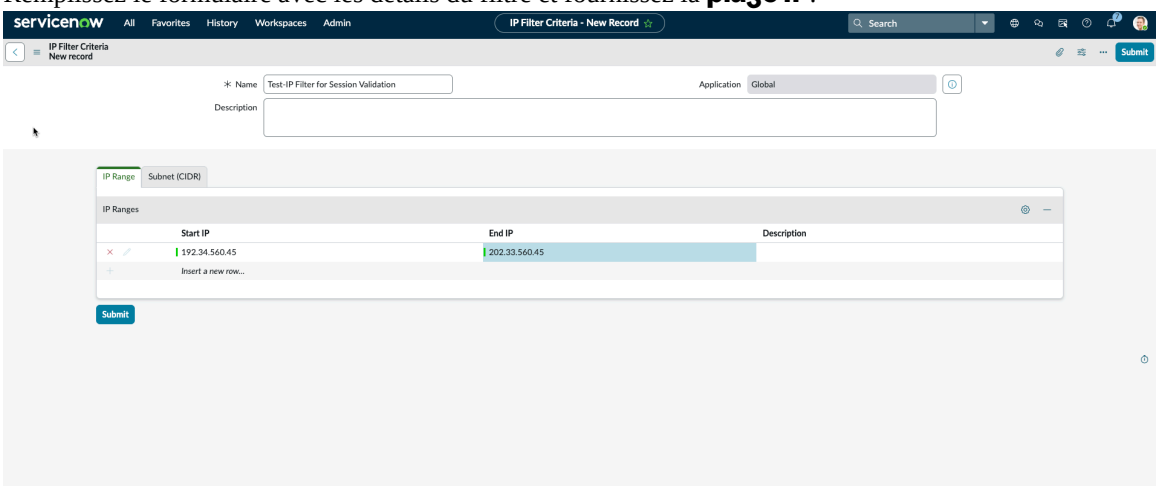
Pour configurer la validation de session, vous devez procéder comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Sélectionnez la **politique de validation de session** dans la page Politiques (sys_authentication_policy_list.do).
3. **Sélectionnez Entrées de politique**.
   a. Sélectionnez **Nouveau** ou **Modifier**.
   b. Choisissez le type d'entrée de politique (critères de filtrage) que vous souhaitez créer.
   Les options disponibles sont les suivantes : adresse IP, rôle et critères de filtre de groupe. Choisissons **Critères de filtre IP**.
   c. Remplissez le formulaire avec les détails du filtre et fournissez la **plage IP**.



Pour en savoir plus sur la création d'un filtre IP, reportez-vous à la section Créer un critère de filtre d'adresses IP.

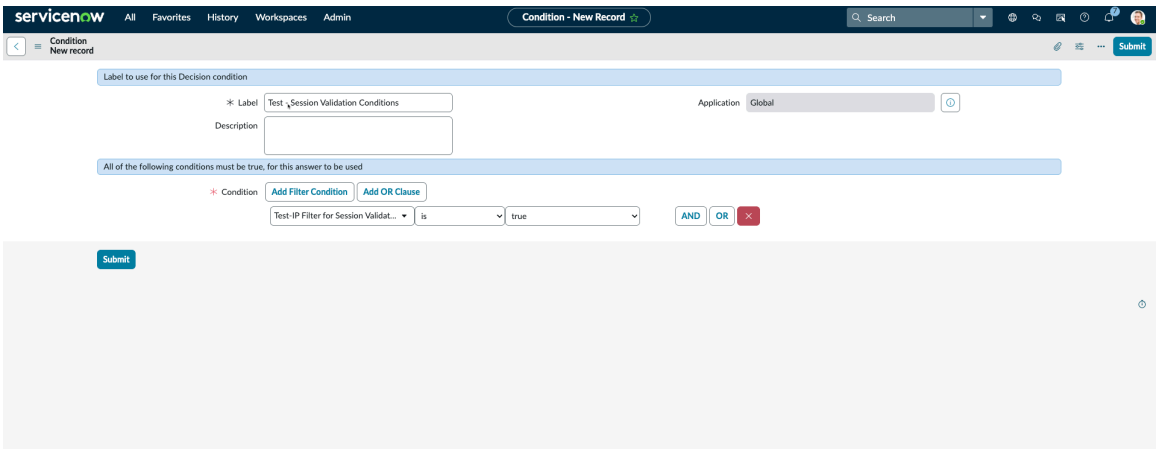
   d. Sélectionnez **Soumettre**.
4. Sélectionnez **Conditions de politique** sur la page Politique de validation de session.
   a. Sélectionnez **Nouveau**.
   b. Remplissez le formulaire et définissez la condition pour l'entrée de politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Vous pouvez définir les conditions sur `vrai` ou `faux` en fonction de la configuration de l'entrée de politique. Dans cet exemple, elle est définie sur `vrai`. Dans ce cas, la définition de la condition sur vrai permet uniquement à l'utilisateur avec l'adresse IP configurée de se connecter.



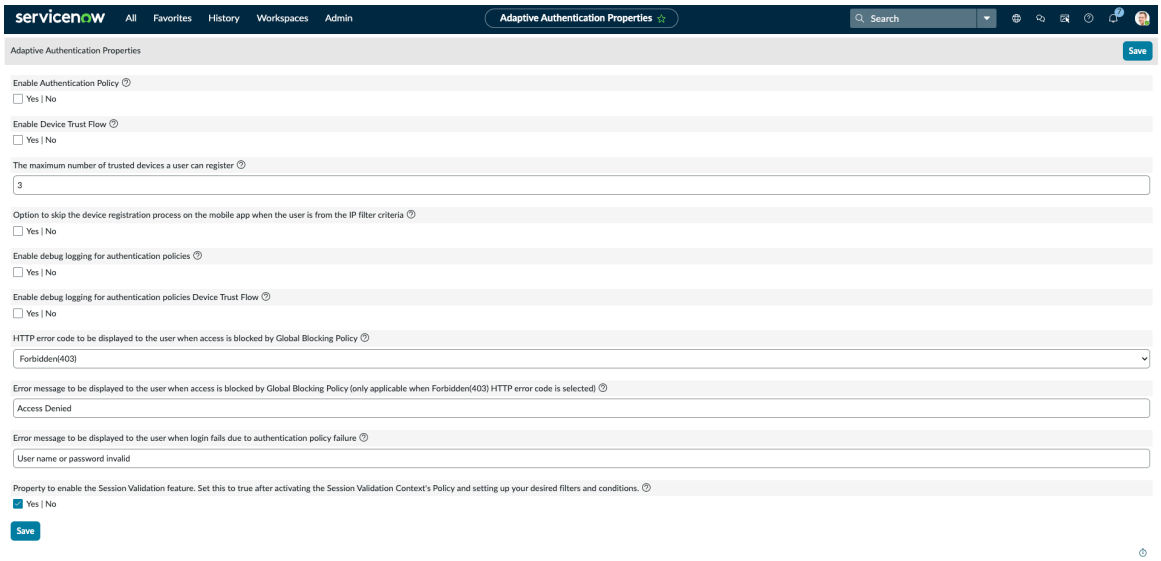
5. Cochez la case `Actif` pour activer la politique une fois que la politique de validation de session est configurée avec les entrées et les conditions de la politique.



6. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés** et activer la propriété Validation de session.

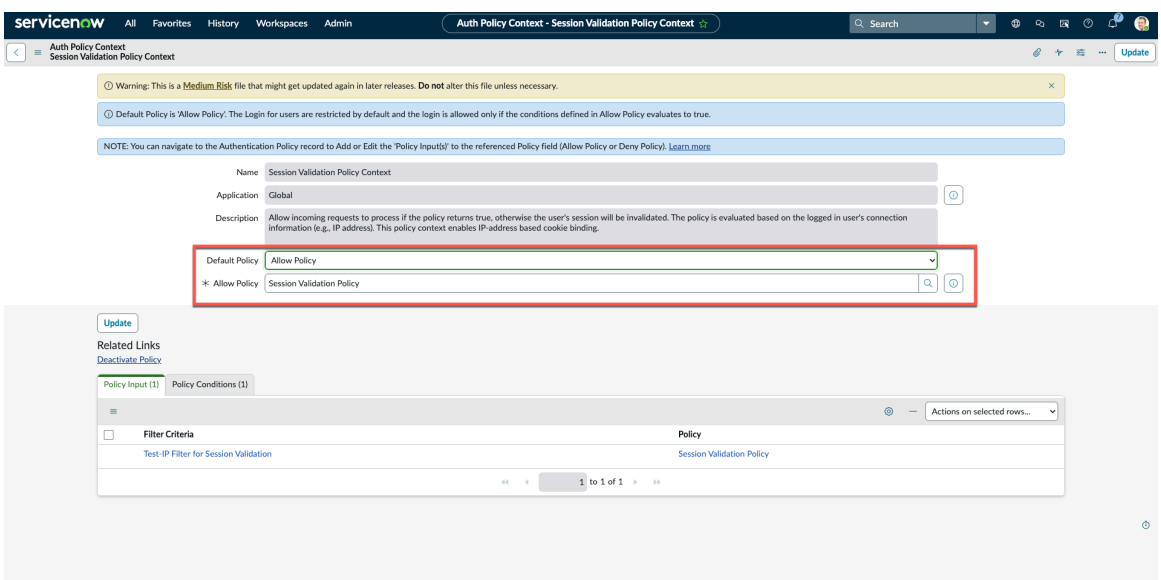
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de validation de la session**.
8. Définissez la politique par défaut sur **autoriser la politique** ou refuser la **politique** pour définir le contexte de validation de session en fonction de l'entrée et des conditions de la politique.

> **Remarque :**
> Par défaut :
>
> - Le contexte de validation de session est défini sur **Autoriser la politique**.
> - La politique d'autorisation est sélectionnée en tant que **politique de validation de session**.



Résultats

La configuration évalue la session de connexion en fonction des éléments suivants :

- Restreint l'accès à l'instance lorsque les ServiceNow® pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité d'une session.
- Restreint l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques d'authentification

Les politiques d'authentification évaluent les demandes d'authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l'accès en fonction du résultat de l'évaluation des conditions de politique. Par exemple, l'accès n'est autorisé que si toutes les conditions de politique spécifiées dans la **politique d'accès** sont évaluées comme vraies.

Utilisez les politiques d'authentification intégrées ou créez une politique d'authentification en fonction de vos besoins de sécurité. Vous pouvez trouver les politiques sur votre instance en accédant à **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.

Remarque :
À tout moment, la politique d'accès d'autorisation ou de refus d'accès peut être exécutée, mais pas les deux.

Politique	Description
Autoriser la politique d'accès	Refuse toutes les demandes d'authentification par défaut. Autorise uniquement les demandes d'authentification qui correspondent aux conditions de politique spécifiées.
Autoriser la politique de pré-authentification	Autoriser la politique de pré-authentification.
Autoriser les utilisateurs à connexion non locale	Choisissez cette politique pour autoriser les utilisateurs à connexion non locale. Utilisé dans le contexte des flux de récupération SSO.
Refuser la politique d'accès	Autorise les demandes d'authentification par défaut. Refuse uniquement les demandes d'authentification qui correspondent aux conditions de politique spécifiées.
Politique de blocage globale	Refuse les demandes d'accès des utilisateurs et des API avant l'authentification. Cette politique peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.
Politique de validation de session	La politique d'authentification évalue les critères de filtre (par exemple, l'adresse IP) pour déterminer si une session doit rester active pour les demandes entrantes. Vous devez définir les critères de filtre sur cette politique.
Politique de refus de connexion locale	Choisissez cette politique pour bloquer toutes les connexions locales. Utilisé dans le contexte des flux de récupération SSO.
Politique MFA descendante	Choisissez **la politique MFA descendante** comme politique par défaut dans les situations où les utilisateurs n'ont pas besoin d'authentification MFA. Lorsque les conditions de politique définies dans la politique de MFA ascendante sont évaluées comme vraies, les utilisateurs ne sont pas tenus de se connecter à l'aide de la MFA.
Politique MFA ascendante	Choisissez **la politique MFA** ascendante comme politique par défaut pour exiger l'authentification MFA lorsque les conditions de politique définies dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique	Description
	la politique MFA ascendante sont évaluées comme vraies.

Configurer une politique d'authentification

Configurez une politique d'authentification pour définir les entrées et les conditions à utiliser pour accorder l'accès à une instance ou appliquer l'authentification multifacteur.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.

   Remarque :
   Pour afficher des exemples de politiques terminées, vous pouvez examiner ces politiques sur votre instance :

   - POLITIQUE DE DÉMO : autoriser la connexion locale pour les administrateurs à partir de la plage d'adresses IP de confiance uniquement
   - POLITIQUE DE DÉMO : autoriser la connexion locale pour les administrateurs uniquement
   - POLITIQUE DE DÉMO : restreindre l'authentification basée sur nom d'utilisateur et mot de passe pour des utilisateurs spécifiques

2. Cliquez sur le bouton **Nouveau** pour créer un enregistrement de politique.
3. Renseignez les champs du formulaire **Politique** .

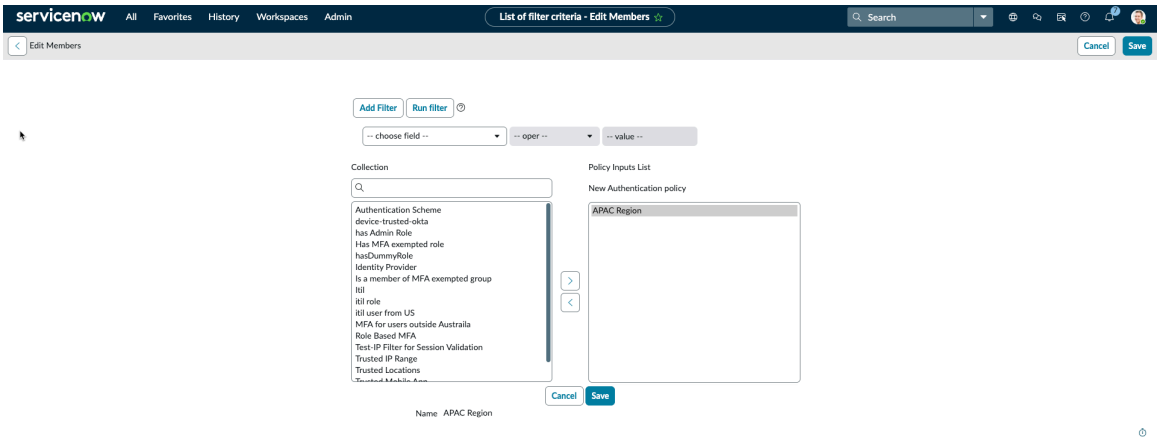
   Formulaire de police

Champ	Description
Nom	Nom de votre police.
Application	Application incluse dans le périmètre de la politique. Ce champ est renseigné automatiquement avec l'application actuelle.
Description	Description de la politique
Actif	Indique si la politique est active.

4. Dans l'onglet **Entrées de politique** , cliquez sur **Modifier**.
5. Sélectionnez un ou plusieurs critères de filtre **dans la liste** Collection et déplacez-les vers **Liste d'entrées de politique** de la liste de **politique d'autorisation d'accès** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Pour plus d'informations sur la création de vos propres critères de filtre à utiliser dans cette section, reportez-vous à la section Critère de filtre.

6. Dans l'onglet **Conditions de la politique** , cliquez sur **Nouveau**.
7. Renseignez les champs suivants du formulaire :

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtre) utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires à partir d'une liste d'adresses IP de confiance.

8. **Facultatif :** Répétez l'étape 7 pour créer des conditions de politique supplémentaires.

Remarque :
Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la politique sera évaluée comme vraie si l'une de vos conditions de police est remplie.

9. Cliquez sur **Enregistrer**.

Ajouter une politique d'authentification à un contexte de politique d'authentification

Ajoutez une politique d'authentification à l'un des contextes de politique d'authentification. Le contexte d'authentification utilise les entrées et les conditions de la politique pour déterminer si les utilisations ont accès à l'instance ou si la MFA est appliquée pour vos utilisateurs.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification**et sélectionnez l'une des entrées en fonction de vos besoins.

   Contexte de pré-authentification

   Utilisez le contexte de pré-autorisation pour évaluer votre politique avant que l'utilisateur ne voie l'écran de connexion. L'accès est accordé ou refusé aux utilisateurs en fonction de cette évaluation.

   Contexte de post-authentification

   Utilisez le contexte de post-autorisation pour évaluer votre politique une fois que l'utilisateur a entré ses informations d'identification de connexion. L'accès est accordé ou refusé aux utilisateurs en fonction de cette évaluation. Étant donné que cette évaluation a lieu après que l'instance a identifié l'utilisateur, les politiques dans ce contexte peuvent effectuer leur évaluation en fonction des données de l'utilisateur, telles que son rôle ou son groupe.

   Contexte MFA

   Utilisez le contexte MFA pour déterminer si un utilisateur doit utiliser l'authentification multifacteur lors de la connexion.

   Contexte de validation de la session

   Utilisez le contexte de validation de session pour évaluer l'adresse IP qui est définie en fonction des conditions définies comme filtre et qui autorise l'accès à l'instance au sein d'une session.

2. Dans le champ **Politique par défaut** , sélectionnez une valeur.
   La valeur de ce champ détermine la façon dont le contexte utilise le résultat des conditions de votre politique.

   Les options disponibles dans ce champ dépendent du contexte sélectionné. Pour plus d'informations sur ces contextes, reportez-vous à la section Contextes de la politique d'authentification.

3. Affectez une politique au contexte.
   Le nom du champ dépend du contexte que vous avez sélectionné.

   Contexte de pré-authentification et de post-authentification

   Ces contextes disposent d'un champ **Politique de refus** ou **Politique d'autorisation** , en fonction de la sélection dans le champ **Politique par défaut** .

   Contexte MFA

   Ce contexte dispose d'un champ **Politique MFA ascendante** ou **Politique MFA descendante** , en fonction de la sélection dans le champ **Politique par défaut** .

   Contexte de validation de session

   Ce contexte dispose d'un champ **Autoriser la politique** ou **Refuser la politique** , en fonction de la sélection dans le champ **Politique par défaut** .

4. Cliquez sur **Mettre à jour**.
   Après la mise à jour de l'enregistrement, vous pouvez voir les entrées et les conditions de votre politique dans les onglets **Entrée de politique** et **Conditions de politique** .

Événements d'authentification adaptative

Vous pouvez utiliser la table d'événements d'authentification adaptative pour en savoir plus sur les événements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici quelques-uns des journaux qui peuvent être suivis dans la table des événements d'authentification adaptative :

- glide.adaptive.auth.log.success.event : pour connaître les événements de réussite pour l'authentification post-utilisateur, connexions API.
- glide.adaptive.auth.log.mfa.relax.event : pour connaître les événements mfa_relaxation pour le contexte MFA.

Remarque :

- Pour le contexte de pré-authentification, les politiques d'accès de l'API REST de type « pre_auth » : par défaut, les événements de défaillance sont consignés. Les événements de réussite ne peuvent pas être consignés.
- Pour le contexte de post-authentification, les politiques d'accès de l'API REST d'un type autre que « pre_auth » : par défaut, événements d'échec ou consignés. Pour que les événements de réussite soient enregistrés, vous devez activer la propriété glide.adaptive.auth.log.success.event .
- Pour la MFA : par défaut, les événements d'application de la MFA sont journalisés.
- Pour que les événements de relaxation MFA soient enregistrés, vous devez activer la propriété glide.adaptive.auth.log.mfa.relax.event . L'assouplissement de la MFA consignerait le même événement que l'application de la MFA, mais avec le champ de résultat renseigné avec la valeur Faux.

Configurer les propriétés d'authentification adaptative

Après avoir activé l'authentification adaptative, configurez les propriétés d'authentification adaptative en fonction de vos besoins de sécurité.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
2. Configurez ces propriétés :

Propriétés d'Authentification adaptative

Propriété	Description	Valeur
Activer la politique d'authentification (glide.authenticate.auth.policy.enabled)	Option permettant d'activer la politique d'authentification.	Oui | Non
Activer la journalisation de débogage pour les politiques d'authentification (glide.authenticate.policy.debug)	Option permettant d'activer la journalisation de débogage pour les stratégies d'authentification.	Oui | Non
Code d'erreur HTTP à afficher l'utilisateur lorsque l'accès est bloqué par la politique de blocage globale (glide.authenticate.global.blocking_policy.error_code)	Code d'erreur HTTP qui s'affiche pendant la connexion lorsque la politique de blocage globale bloque la connexion d'un utilisateur.	Sélectionner à partir de : ○ Interdit(403) ○ Introuvable(404)
Message d'erreur à afficher à l'utilisateur lorsque l'accès est bloqué par la politique de blocage globale (applicable uniquement si le code d'erreur HTTP	Message d'erreur qui s'affiche lorsque la politique de blocage globale bloque l'accès.	Champ de texte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur
403 « Forbidden » est sélectionné) (glide.authenticate.global.blocking_policy.error_message)		
Activer le flux de confiance d'appareil (glide.authenticate.preauth.allow.trusted.device)	Option permettant d'activer le flux d'appareils de confiance.	Oui | Non
Nombre maximal d'appareils de confiance qu'un utilisateur peut enregistrer (glide.trusted.device.max.count)	Il s'agit du nombre maximal d'appareils de confiance qu'un utilisateur peut enregistrer.	Champ de texte
Ignorer l'inscription de l'appareil pour le flux de confiance de l'appareil si l'utilisateur provient d'un réseau approuvé (glide.authenticate.preauth.skip.user.registration)	Option permettant d'ignorer l'inscription si l'utilisateur essaie de s'inscrire à partir du réseau approuvé	Oui | Non
Propriété permettant d'activer la fonctionnalité Validation de session. Définissez-le sur vrai après l'activation de la politique du contexte de validation de session et la configuration des filtres et conditions souhaités (session.validation.enabled)	Option permettant d'activer la fonctionnalité Validation de session. Définissez cette valeur sur vrai après avoir activé la politique du contexte de validation de session et configuré les filtres et conditions souhaités.	Oui | Non

Didacticiel : Configurer l'authentification adaptative

Utilisez ces exemples d'étapes pour configurer l'authentification adaptative sur une instance.

Pour utiliser ce didacticiel, vous devez disposer d'une instance sur laquelle l'authentification adaptative est activée. Pour obtenir des détails sur ce processus, consultez Activer l'authentification adaptative.

L'exemple vous guide dans la création d'une nouvelle stratégie et son application à une instance. Dans ce didacticiel, vous allez :

Créer un enregistrement de critère de filtre

Créez un enregistrement de critères de filtre de groupe à utiliser comme entrée dans votre politique. Cet enregistrement permet à votre politique de déterminer l'accès en fonction du groupe d'utilisateurs. Au cours de ces étapes, vous définissez le ou les groupes que la politique utilise pour déterminer l'accès.

Créer une politique

Créez une politique qui détermine si un utilisateur peut accéder à l'instance. Cette politique utilise l'enregistrement de critères de filtre de groupe que vous créez comme entrée. Au cours de ces étapes, vous définissez également des conditions de politique qui définissent la façon dont la politique utilise l'entrée de politique pour déterminer l'accès des utilisateurs.

Configurer un contexte de politique

Configurez le **contexte de politique de post-authentification** pour utiliser votre nouvelle politique. Lorsqu'elle est configurée, votre instance refuse l'accès aux utilisateurs du groupe défini dans l'enregistrement des critères de filtre.

Créer un enregistrement de critère de filtre

Découvrez comment créer un enregistrement de critères à utiliser comme entrée de politique pour votre politique d'authentification adaptative.

Avant de commencer

Rôle requis : admin

Traduction automatique

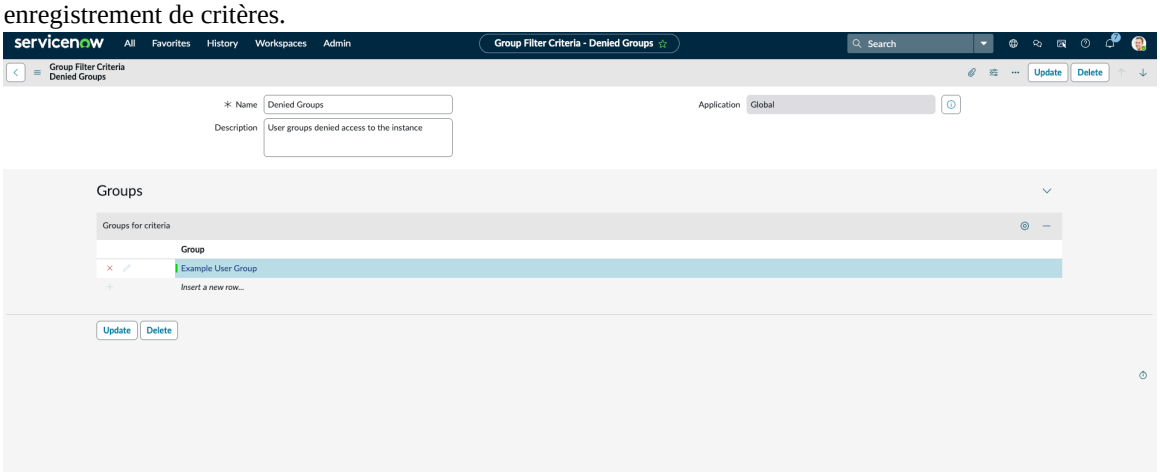
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour refuser l’accès à votre instance en fonction des groupes d’utilisateurs, vous devez créer un enregistrement de critères de filtre de groupe. Cet enregistrement définit un groupe d’utilisateurs ou un ensemble de groupes d’utilisateurs auxquels votre politique peut accorder ou refuser l’accès. Dans cet exemple, vous allez créer un enregistrement de critère de filtre de groupe pour un seul groupe d’utilisateurs.

Pour en savoir plus sur les groupes d’utilisateurs et leur utilisation dans votre instance, reportez-vous à la section Exploring user administration .

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critères de groupe**.
2. Cliquez sur **Nouveau** et créez un enregistrement.
3. Dans le champ **Nom** , saisissez un nom pour votre enregistrement.
   Par exemple, Groupes refusés.
4. Dans le champ **Description** , saisissez une brève description.
   Par exemple, des groupes d’utilisateurs ont refusé l’accès à l’instance.
5. Dans la liste **Grouper pour les critères** , double-cliquez sur **Insérer une nouvelle ligne...**.
6. Entrez le nom d’un groupe d’utilisateurs ou cliquez sur l’icône de référence (icône de) pour sélectionner un groupe dans une liste.
   Si vous souhaitez créer un nouveau groupe d’utilisateurs pour vos critères de filtrage, cliquez sur l’icône de référence ( ), puis cliquez sur le bouton **Nouveau** . Pour plus de détails sur la création de groupes d’utilisateurs, voir Créer un groupe d’utilisateurs .
7. Une fois que vous avez ajouté votre groupe d’utilisateurs, cliquez sur **Envoyer** pour sauvegarder votre enregistrement de critères.



Créer une politique

Découvrez comment créer une politique pour refuser l’accès aux groupes d’utilisateurs définis dans vos critères de filtre de groupe.

Avant de commencer

Rôle requis : admin

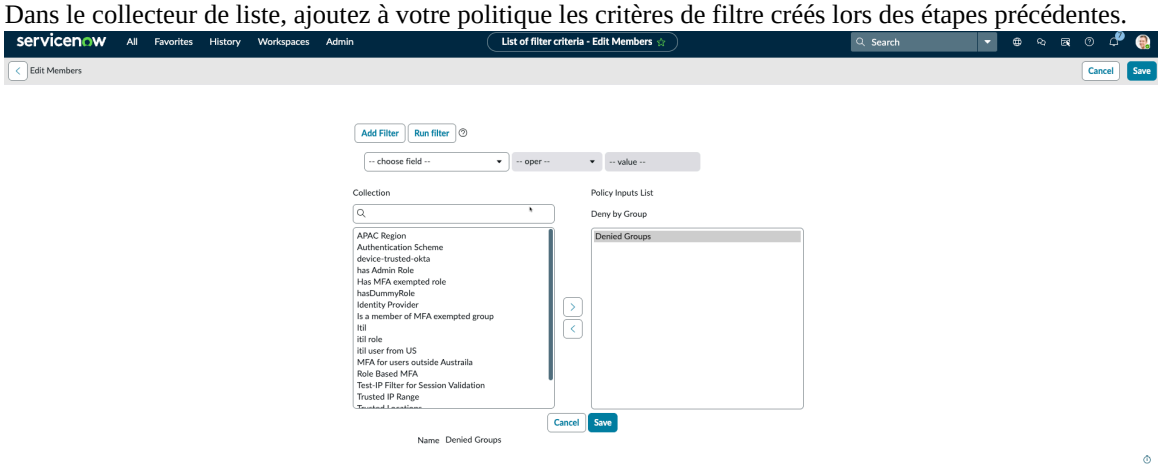
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Dans la liste **Politiques** , cliquez sur **Nouveau**.

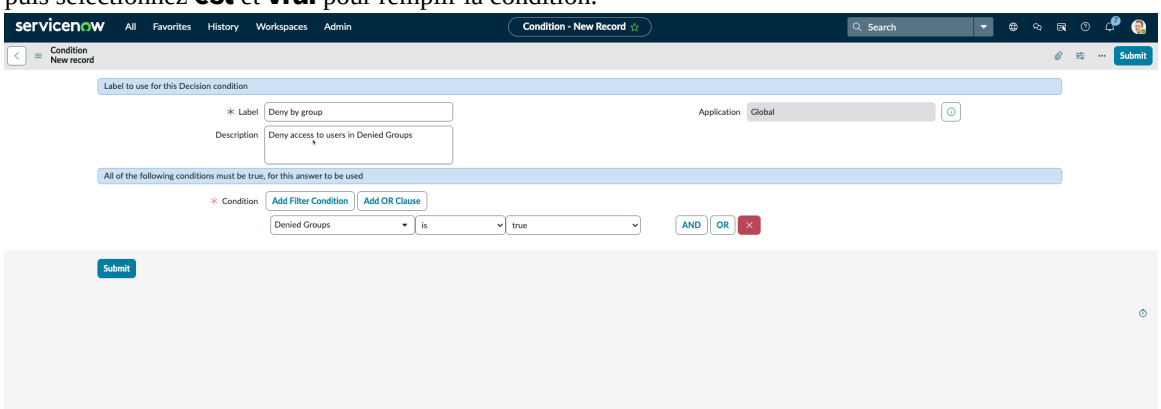
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans le champ **Nom** , saisissez un nom pour votre enregistrement.
   Par exemple, Refuser par groupe.
4. Dans le champ **Description** , saisissez une brève description.
   Par exemple, des groupes d'utilisateurs ont refusé l'accès à l'instance.
5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
   Après l'enregistrement, les listes **Entrées** de **politique et Conditions de politique** s'affichent sur le formulaire.
6. Dans la liste **Entrées de politique** , cliquez sur **Modifier**.
7. Dans le collecteur de liste, ajoutez à votre politique les critères de filtre créés lors des étapes précédentes.



8. Cliquez sur **Enregistrer**.
   L'instance enregistre l'entrée de politique et affiche que l'enregistrement de politique s'affiche à nouveau.
9. Dans la liste **Conditions de la politique** , cliquez sur **Nouveau**.
10. Dans le champ **Étiquette** , créez une étiquette pour cette condition, par exemple Refuser par groupe.
11. Dans le champ **Description** , saisissez une brève description.
    Par exemple, Refuser l'accès aux utilisateurs des groupes refusés.
12. Dans le champ **Condition** , sélectionnez les critères de filtre que vous avez créés lors des étapes précédentes, puis sélectionnez **est** et **vrai** pour remplir la condition.



13. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un contexte de politique

Configurez le contexte de politique de post-authentification pour utiliser votre nouvelle politique. Lorsqu'elle est configurée, votre instance refuse l'accès aux utilisateurs du groupe défini dans l'enregistrement des critères de filtre.

Avant de commencer
Rôle requis : admin

Procédure

1. **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de post-authentification**.
   Vous devez utiliser le **contexte de post-authentification** , car la stratégie utilisée dans ce didacticiel doit évaluer le groupe dans lequel se trouve un utilisateur. Ces informations ne sont disponibles qu'après la saisie de leurs informations d'identification.
2. Dans le champ **Politique par défaut** , sélectionnez Refuser la politique.
   Cette sélection accorde l'accès aux utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions de politique sont évaluées comme vraies.
3. Dans le champ **Refuser la politique** , sélectionnez la politique que vous avez créée aux étapes précédentes.
4. Cliquez sur **Mettre à jour** pour enregistrer l'enregistrement du contexte de la politique.

Authentification adaptative pour les applications mobiles de confiance

Accédez à vos ServiceNow réseaux à partir de réseaux non approuvés à l'aide du Application Now Mobile.

Authentification adaptative pour les applications mobiles de confiance

L'authentification adaptative pour les applications mobiles de confiance permet aux utilisateurs d'accéder à l'instance ServiceNow à l'aide du Application Now Mobile. L'instance est protégée derrière une limite de réseau IP approuvée.

Voici quelques-uns des scénarios dans lesquels vous avez besoin d'accéder à l'instance lorsque vous êtes en dehors de votre réseau.

En tant qu'employé, vous devez accéder au Centre de services aux employés (portail) depuis l'extérieur Application Now Mobile du réseau. Le filtre d'application mobile approuvée vous permet d'identifier la demande entrante provenant d'une application Application Now Mobile approuvée liée à un compte d'utilisateur.

En tant qu'administrateur, vous pouvez configurer la politique. La politique permet aux utilisateurs d'enregistrer leurs équipements mobiles et d'accéder à l'instance sur un réseau approuvé.

En tant qu'utilisateur, vous pouvez enregistrer votre appareil mobile en scannant le code QR affiché sur l'instance. Après l'inscription, vous pouvez vous connecter à votre instance à partir du , à l'aide de vos informations d'identification Application Now Mobile.

Remarque :
Pour enregistrer l'appareil mobile, vous devez être sur un réseau de confiance. Après l'inscription, vous pouvez également vous connecter à l'instance à partir d'autres réseaux.

Fonctionnalités

En tant qu'administrateur, vous pouvez utiliser les fonctionnalités suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurez les politiques à l'aide des critères de filtre d'application approuvés.
- Créez des conditions de politique avec un nouveau critère de filtre pour les applications mobiles de confiance.
- Prenez en charge toutes les méthodes de connexion sur l'application mobile de confiance pour les utilisateurs (connexion locale, SAML, OIDC et MFA).
- Révoquer un appareil approuvé.
- Ajoutez des événements de sécurité pour toutes les actions d'enregistrement ou de révocation de l'appareil. Les événements peuvent être utilisés pour notifier l'utilisateur.
- Prenez en charge les événements de sécurité pour les échecs de signature, les échecs de validation des cookies, les jetons non valides, les en-têtes non valides ou les paramètres de requête.
- Contrôlez le nombre maximal d'appareils enregistrés.
- Empêchez l'enregistrement d'un nouvel appareil, sauf si l'utilisateur supprime un appareil déjà couplé.
- Capturez la dernière fois qu'un appareil a été utilisé.

Activer l'application mobile de confiance

Activez l'authentification adaptative avec l'application mobile de confiance à l'aide de la politique d'authentification et des conditions de filtre.

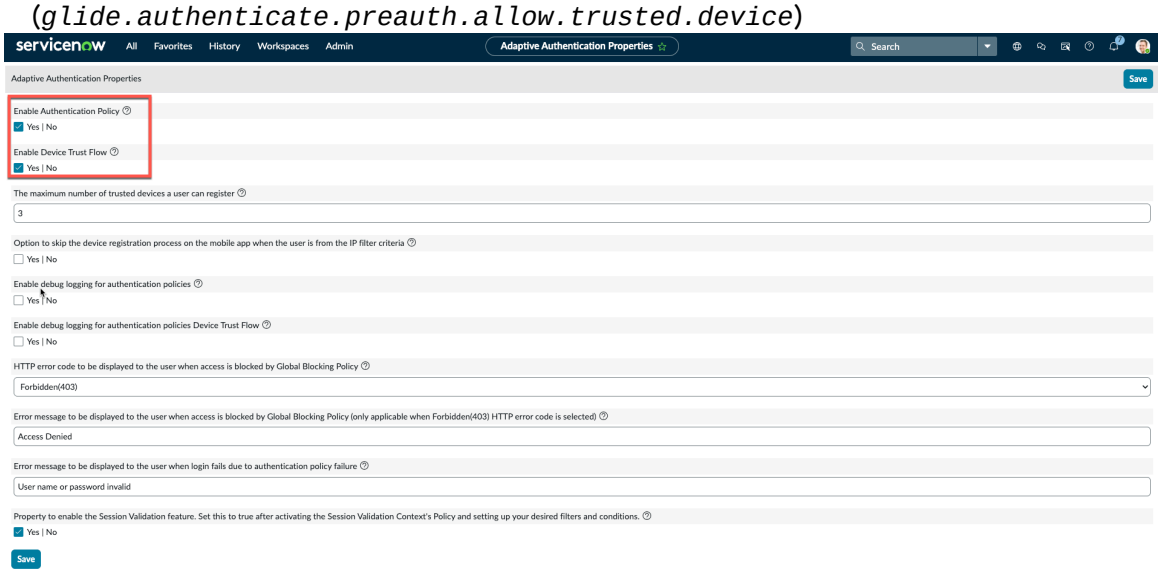
Avant de commencer

Assurez-vous que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) est installé.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
2. Sur la page Propriétés d'Authentification adaptative, activez les propriétés suivantes :
   - Activer la politique d'authentification (`glide.authenticate.auth.policy.enabled`)
   - Activer le flux de l'appareil de confiance (`glide.authenticate.preauth.allow.trusted.device`)



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

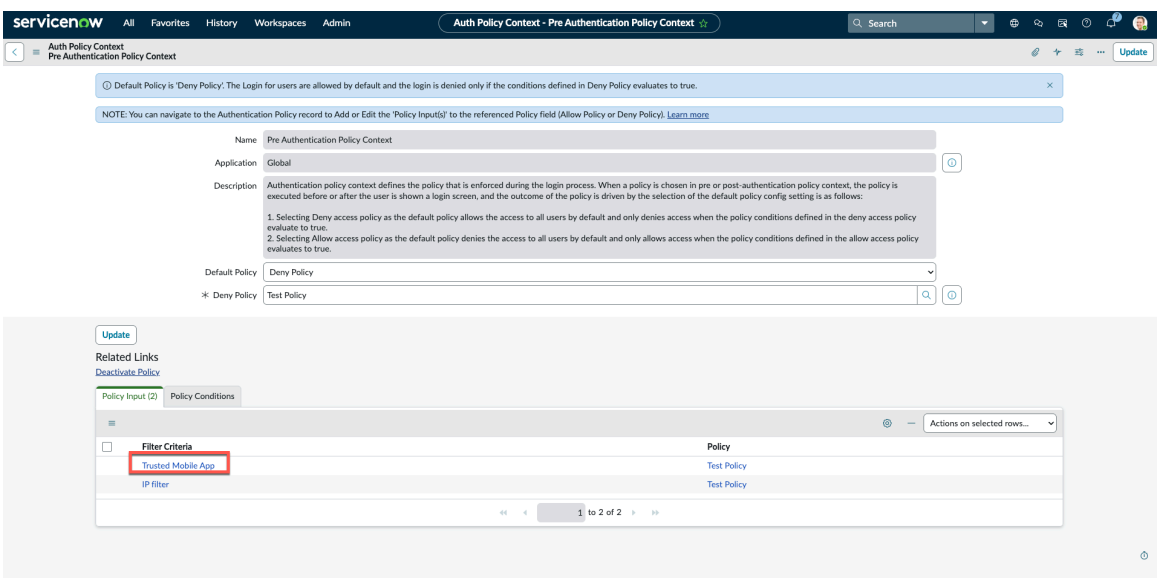
Remarque :
Pour désactiver la propriété de flux de confiance de l'appareil, vous devez supprimer les conditions avec filtre mobile de confiance. Sinon, un message d'erreur s'affiche pour supprimer les conditions.

3. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de pré-authentification**.
4. Définissez les conditions dans le contexte de pré-authentification.
   Pour en savoir plus, Contexte de pré-authentification.

Remarque :
Par défaut, la condition de politique est **Refuser la politique**. Vous pouvez changer en **politique d'autorisation**. Ces politiques sont directement opposées.

- Avec la **politique d'autorisation**, l'accès est refusé par défaut à tous les utilisateurs et elle n'autorise l'accès que lorsque les conditions de la politique d'autorisation d'accès sont vraies.
- Avec la **politique de refus**, tous les utilisateurs sont autorisés à accéder par défaut, et celle-ci ne refuse l'accès que lorsque les conditions de la politique de refus d'accès sont vraies.

Dans l'entrée de politique, l'entrée de politique **de l'application mobile de confiance** est une entrée de politique pour l'application mobile de confiance.



5. Dans les conditions de la politique, créez la condition en cliquant sur **Nouveau**.
6. Renseignez les champs du formulaire.

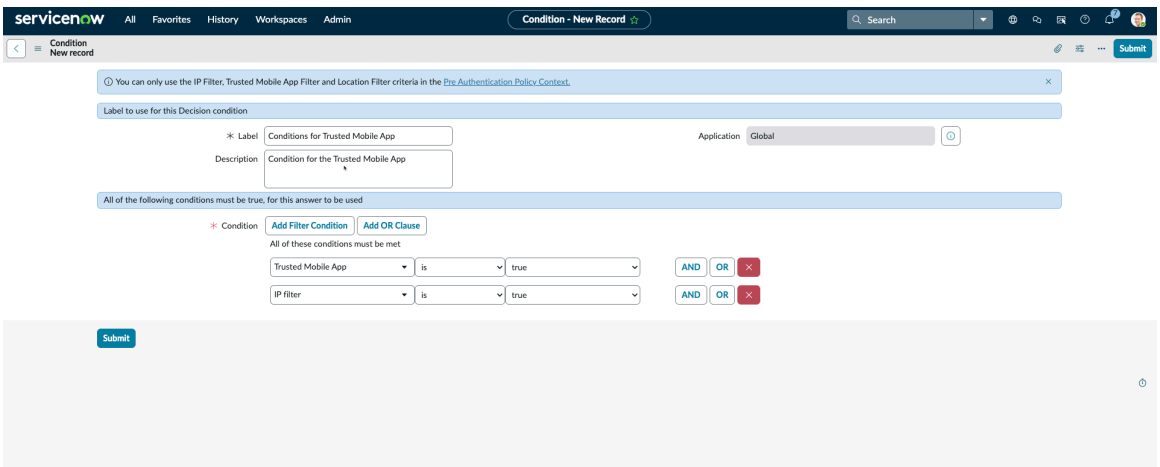
Formulaire de condition de filtre

Champ	Description
Étiquette	Nom de la condition
Description	Description de la condition
Application	Le périmètre de l'application pour cet enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Conditions basées sur ET et OU. Étant donné que la politique d'authentification est **une politique d'autorisation**, la condition pour l'application mobile de confiance est définie sur vrai dans l'exemple affiché sur l'image.



7. Cliquez sur **Envoyer**.

Résultats

L'entrée de politique et les conditions de filtre sont créées pour la fonctionnalité Appareil de confiance. Les utilisateurs peuvent continuer à utiliser la fonctionnalité Appareil de confiance pour accéder à l'instance ServiceNow à partir de réseaux non approuvés à l'aide du Application Now Mobile. Pour plus d'informations, consultez Enregistrer un appareil de confiance.

Enregistrer un appareil de confiance

Enregistrez un appareil de confiance pour accéder à l'instance ServiceNow en dehors du réseau.

Avant de commencer

Vous devez être dans le réseau approuvé pour effectuer l'enregistrement de l'appareil approuvé.

Rôle requis : aucun

Procédure

1. Accédez à l'une des options de menu suivantes :

- Dans le ServiceNow AI Platform, accédez à **Tous** > **Libre-service** > **Mon profil**.

  Remarque :
  Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

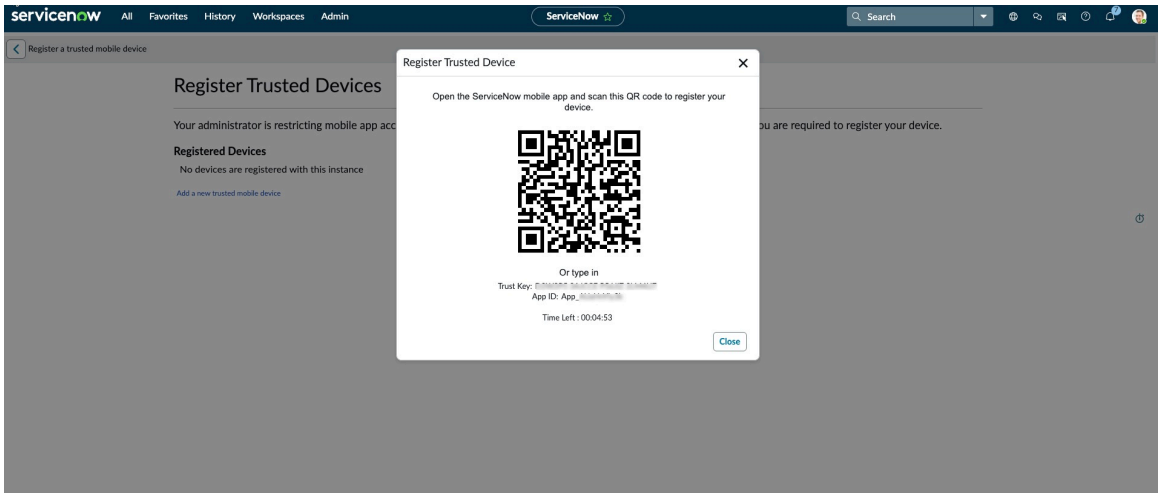
- Dans le Now Support, cliquez sur le profil et sélectionnez **Appareil de confiance**.

2. Dans votre profil d'utilisateur, cliquez sur **Enregistrer un appareil mobile de confiance** dans la section Liens connexes.
La page Enregistrer des appareils de confiance s'affiche.

3. Enregistrez un nouvel appareil en cliquant sur **Ajouter un nouvel appareil mobile de confiance**.

Traduction automatique

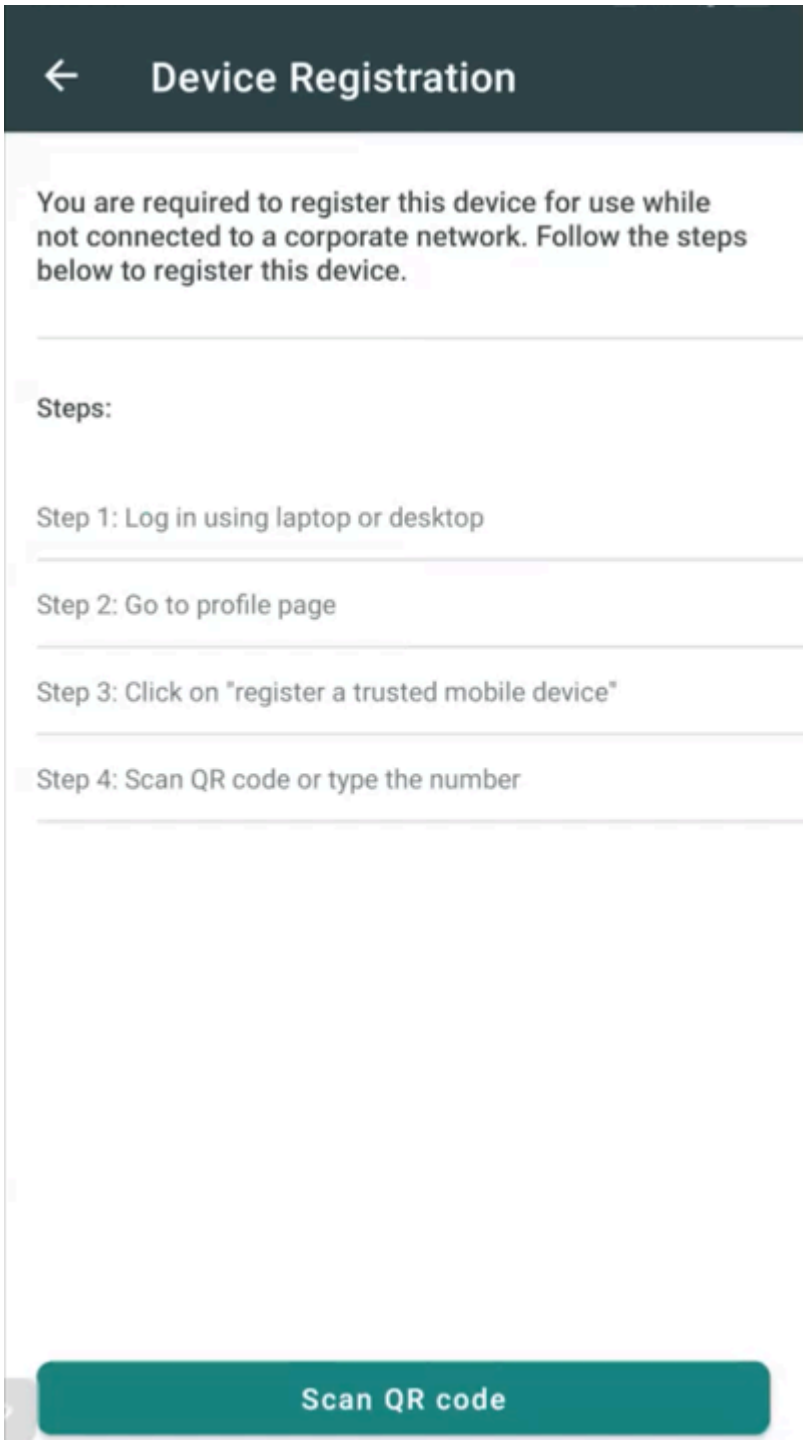
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sur l’écran d’enregistrement de l’appareil de votre ServiceNow application mobile, appuyez sur le bouton **Scanner le code QR** et scannez le code QR qui s’affiche sur votre ordinateur portable ou de bureau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



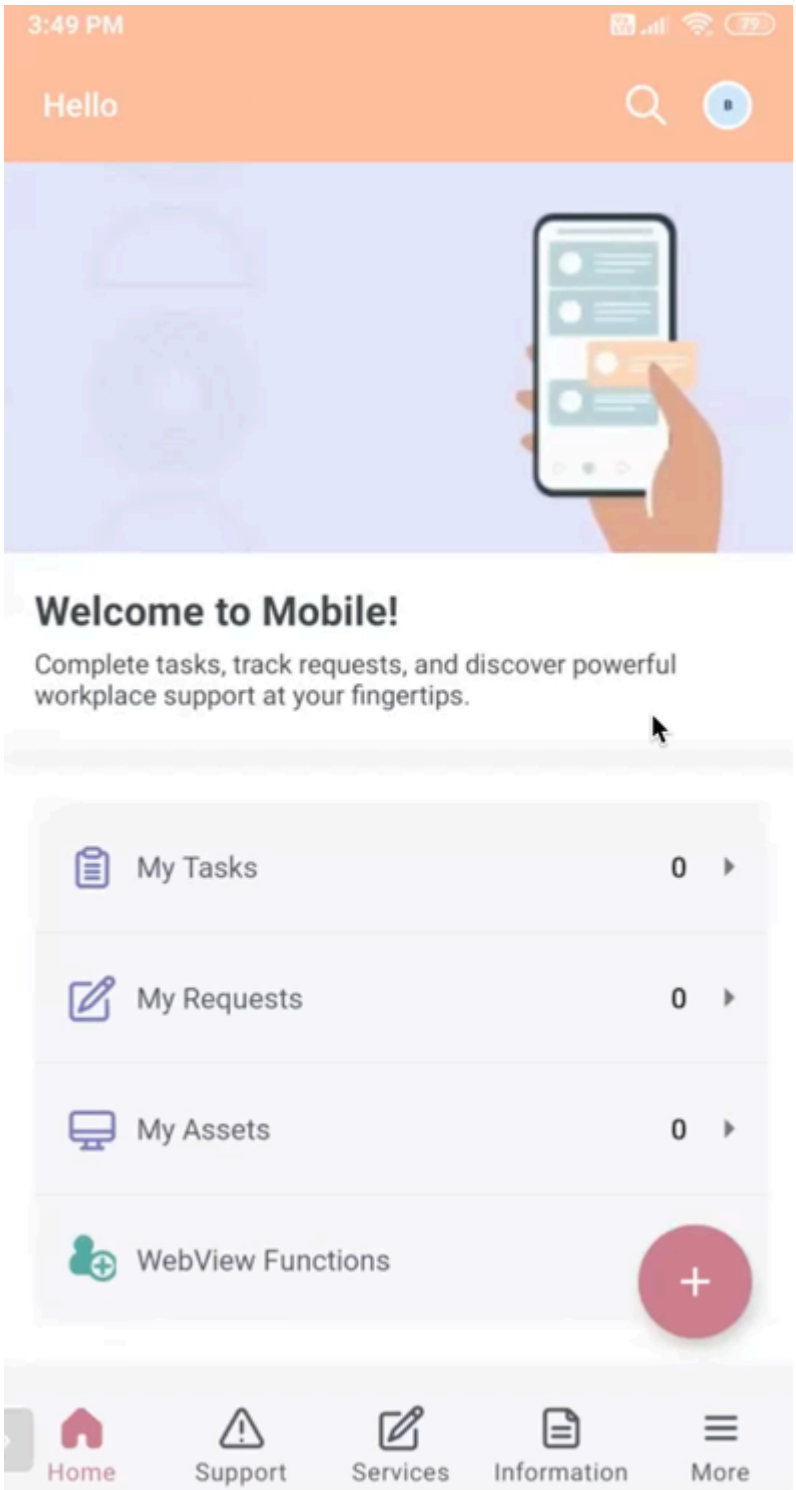
Le processus d’inscription se terminera et vous serez invité à accéder à votre page de connexion pour terminer votre authentification.

5. Indiquez vos informations d’identification Application Now Mobile et connectez-vous au .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’écran de l’accueil mobile s’affiche.



Résultats

La page Enregistrer les appareils de confiance sur votre ordinateur portable ou de bureau affiche l’appareil enregistré. Vous pouvez utiliser l’icône si vous souhaitez supprimer l’appareil enregistré de la page.

Que faire ensuite

Accédez à la **Tous** > **Authentification Adaptative** > **Appareil de confiance** > **Inscription du périphérique** pour afficher tous les détails de l’appareil enregistré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer votre appareil de confiance

Gérez votre appareil de confiance à partir de la page d'enregistrement de l'appareil de confiance.

Avant de commencer

Rôle requis : aucun

Procédure

1. Accédez à l'une des options de menu suivantes :
   - Dans le ServiceNow AI Platform, accédez à **Tous** > **Libre-service** > **Mon profil**.

     Remarque :
     Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

   - Dans le Now Support, cliquez sur le profil et sélectionnez **Appareil de confiance**.
2. Dans votre profil d'utilisateur, cliquez sur **Enregistrer un appareil de confiance** dans la section Liens connexes.
   La page Enregistrer des appareils de confiance s'affiche.
3. Sur la page Enregistrer les appareils de confiance, supprimez l'appareil en cliquant sur l'icône .

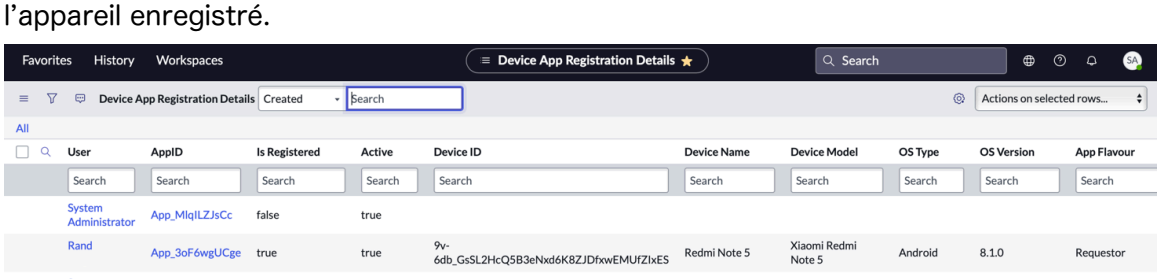
   Remarque :
   L'appareil mobile supprimé doit être enregistré à nouveau pour accéder à l'instance.

Détails d'enregistrement des appareils enregistrés

Affichez les détails des appareils enregistrés auprès de votre ServiceNow instance.

Pour afficher tous les détails de l'appareil enregistré avec l'instance, accédez à **Tous** > **Authentification Adaptative** > **Appareil de confiance** > **Inscription du périphérique**.

Utilisez le filtre pour identifier l'appareil. Cliquez sur le champ **AppID** pour en savoir plus sur l'appareil enregistré.



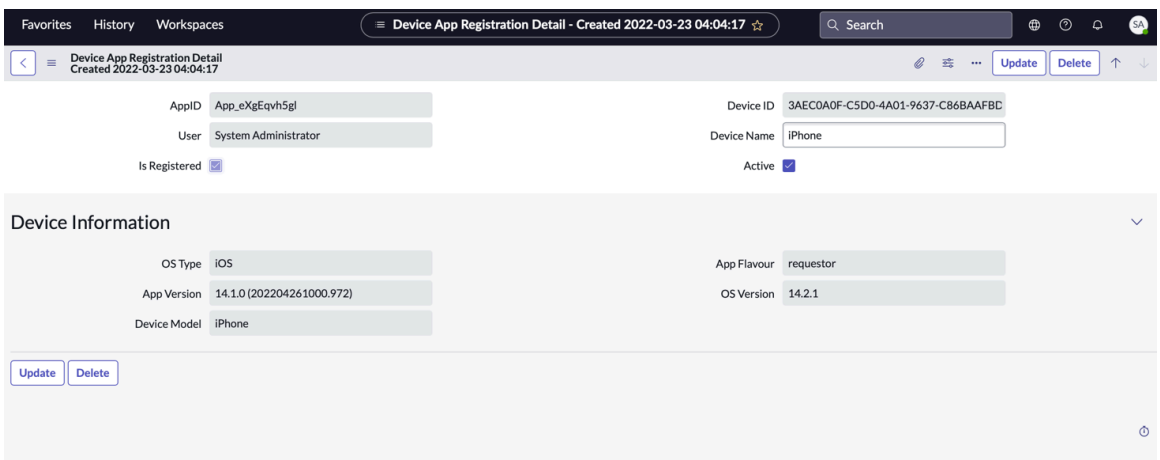
Les détails suivants s'affichent pour l'appareil :

- ID application
- ID d'appareil

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisateur
- Nom de l'équipement
- Informations sur l’appareil, telles que :
  - Type de SE
  - Saveur de l'application
  - Version de l'application
  - Version de SE
  - Modèle d'équipement



Dépannage de l’application mobile de confiance

Passez en revue ces scénarios de dépannage pour résoudre les problèmes de l’application mobile de confiance.

Les sections suivantes décrivent certains scénarios de dépannage et les méthodes de dépannage.

Différence de temps entre l’instance et le mobile (décalage d’horloge)

En cas de décalage d’horloge, vous pouvez ajuster ou réinitialiser l’horloge de votre appareil mobile pour utiliser l’appareil de confiance.

Expiration du code QR dans les cinq minutes

Le code QR pour la fonctionnalité d’appareil de confiance expire dans les cinq minutes. Dans ce cas, vous pouvez cliquer pour obtenir un nouveau code QR.

Remarque :
L’expiration du code QR peut être prolongée. Pour prolonger l’expiration du code, contactez votre administrateur.

La propriété système a changé

Si la propriété système a changé, vérifiez l’inscription en fonction de la propriété système pour les informations d’identification valides pouvant être utilisées pour la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appareil maximum enregistré

Si le nombre maximal d'inscriptions d'appareil est atteint, supprimez l'appareil existant ou contactez votre administrateur pour modifier le nombre maximal d'appareils.

Authentification API

Configurations d'authentification pour l'API.

L'authentification basée sur l'API dans ServiceNow® valide l'identité d'un utilisateur qui accède à une instance, puis autorise l'utilisateur à utiliser les fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur lorsqu'il effectue un appel d'API à l'instance ServiceNow® .

Les types d'authentification API dans sont les ServiceNow® suivants :

- Authentification basée sur certificat
- OAuth
- Authentification basée sur un jeton

Authentification basée sur certificat

L'authentification basée sur certificat vous permet d'authentifier mutuellement les demandes d'API entrantes à l'aide de certificats d'une autorité de certification (CA) approuvée.

Authentification basée sur certificat pour les services Web entrants

Authentifiez les demandes entrantes vers ServiceNow les API SOAP et REST. Pour configurer l'authentification réciproque des services Web entrants, reportez-vous à la section Configurer l'authentification basée sur certificat.

OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance sur le système à l'aide d'un protocole d'authentification.

OAuth 2.0 : autorisation ouverte est le protocole d'autorisation standard de l'industrie, qui s'appuie sur la simplicité des développeurs clients tout en fournissant des flux d'autorisation spécifiques pour les applications Web, les applications de bureau et les équipements mobiles.

Entrant

Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client dont le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section Entrant OAuth.

Authentification basée sur un jeton

Authentification basée sur un jeton pour la configuration des API REST entrantes à l'aide d'une clé API ou HMAC.

Prenez en charge les jetons d'API pour les points de terminaison d'API REST afin que l'authentification ServiceNow® de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'authentification basée sur un jeton pour la configuration des API REST entrantes peut être effectuée sur l'instance avec la clé API ou le ServiceNow® jeton HMAC.

Clé API et authentification HMAC pour les API REST entrantes

Prenez en charge les jetons d'API pour les points de terminaison d'API REST afin que le nom d'utilisateur et le ServiceNow® mot de passe ne soient pas visibles dans l'URL Webhook.

Activez l'authentification basée sur la clé API pour authentifier en toute sécurité l'URL de webhook entrante.

Pour utiliser la clé API et l'authentification HMAC, vous devez installer le (module d'extension : com.glide.tokenbased_auth) dans l'instance ServiceNow® .

⚠ Avertissement :
Utilisez la demande **POST** lors de la soumission d'informations sensibles au serveur.

L'installation de la clé API et de l'authentification HMAC a des dépendances sur les modules d'extension suivants :

- Module d'extension du périmètre d'authentification de l'API REST (com.glide.rest.auth.scope)
- Module d'extension Politique d'accès de l'API REST (com.glide.rest.policy)
- Périmètre d'authentification (com.glide.auth.scope)

Avantages

L'authentification clé API et HMAC pour les API REST entrantes permet :

- Possibilité de spécifier une clé API ou un jeton HMAC pour l'authentification de l'API REST.
- Possibilité d'associer un compte d'utilisateur à la clé API ou au jeton HMAC.
- Possibilité de spécifier un jeton en tant que paramètre de requête ou en-tête dans l'appel d'API REST.
- Possibilité d'associer le périmètre d'authentification aux configurations de clé API ou de jeton HMAC de sorte que les clés API ne puissent être utilisées que pour appeler les API associées à des périmètres particuliers.
- Possibilité d'associer une configuration de clé API ou de jeton HMAC à un profil d'authentification pouvant être utilisé dans les politiques d'accès API.

Activer la clé API et l'authentification HMAC

Vous pouvez activer le module d'extension, la clé API et l'authentification HMAC (com.glide.tokenbased_auth) dans votre ServiceNow® instance.

Avant de commencer
Rôle requis : admin.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez la clé API et le module d'extension d'authentification HMAC (com.glide.tokenbased_auth) à l'aide des critères de filtre et de la barre de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Configurer la clé API : authentification basée sur un jeton

Configurez une clé API pour prendre en charge l'authentification pour les points de terminaison d'API REST.

Avant de commencer
Rôle requis : admin

Module d'extension requis : clé API et authentification HMAC (com.glide.tokenbased_auth)

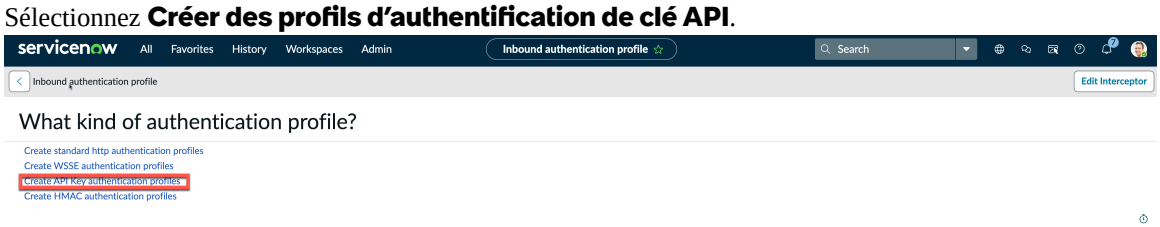
Procédure

1. Créez un profil d'authentification entrant.

   a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.

   b. Sélectionnez **Nouveau**.
   Le système affiche le message Quel type de profil d'authentification ?

   c. Sélectionnez **Créer des profils d'authentification de clé API**.



   d. Remplissez les champs du formulaire.

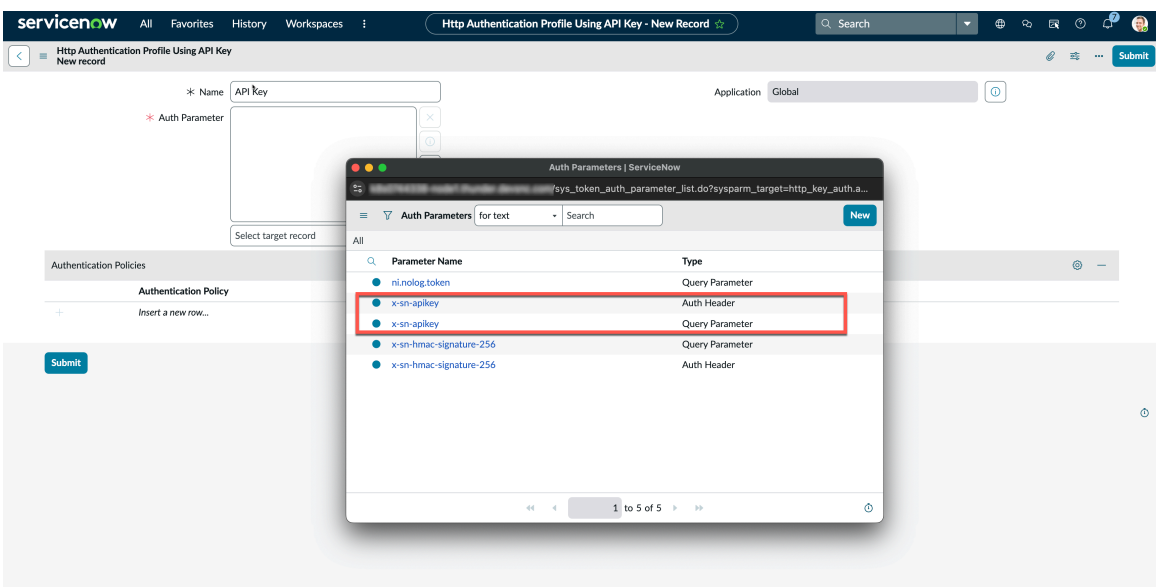
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Profils d'authentification de clé API

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Paramètre d'authentification	Sélectionnez le paramètre d'authentification de la demande d'authentification. Vous pouvez sélectionner les options par défaut ou créer un nouveau paramètre d'authentification : ▪ x-sn-apikey : en-tête d'authentification ▪ x-sn-apikey : en-tête du paramètre de requête

Remarque :
L'option sélectionnée doit être définie dans l'appel REST dans l'en-tête d'authentification ou le paramètre de requête.



Remarque :
Si vous souhaitez ajouter un préfixe pour la clé API, ouvrez le fichier de paramètres d'authentification que vous avez sélectionné et spécifiez le champ **Préfixe** .

e. Envoyez le formulaire.

2. Créez une clé API REST.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Clé API REST**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire :

Traduction automatique

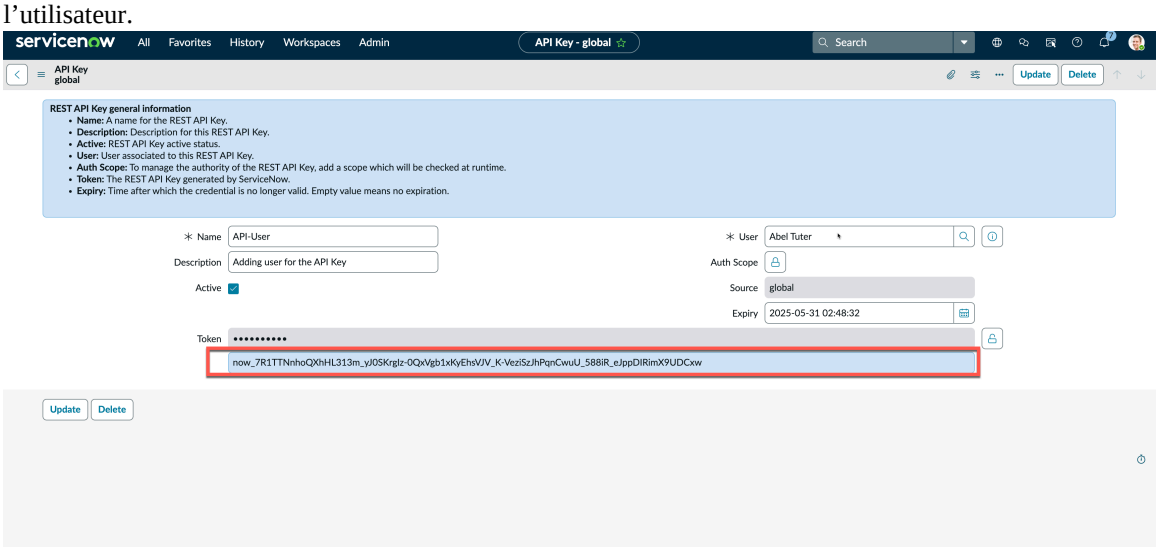
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clé API

Champ	Description
Nom	Nom permettant d'identifier la clé API REST
Description	Description de la clé API REST.
Actif	État de la clé API REST.
Utilisateur	Utilisateur associé à la clé API REST. Utilisez l'icône de recherche pour sélectionner l'utilisateur.
Périmètre d'authentification	Option permettant d'ajouter un périmètre d'authentification pour gérer l'autorité de la clé API REST.
Jeton	Clé API REST générée par le ServiceNow AI Platform fichier . Copiez la clé à utiliser dans le cadre de l'appel d'API REST dans le paramètre En-tête ou Requête.
Expiration	Heure après laquelle les informations d'identification ne sont plus valides. Une valeur vide signifie qu'il n'y a pas d'expiration. **Remarque :** Pour plus d'informations sur l'expiration du jeton, reportez-vous à la section Nettoyage de l'expiration du jeton .

d. Envoyez le formulaire.

e. Ouvrez l'enregistrement qui a été créé pour afficher le jeton généré par ServiceNow AI Platform pour l'utilisateur.



3. Créez une politique d'accès REST API.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.

b. Sélectionnez **Nouveau**.

c. Remplissez les champs du formulaire.

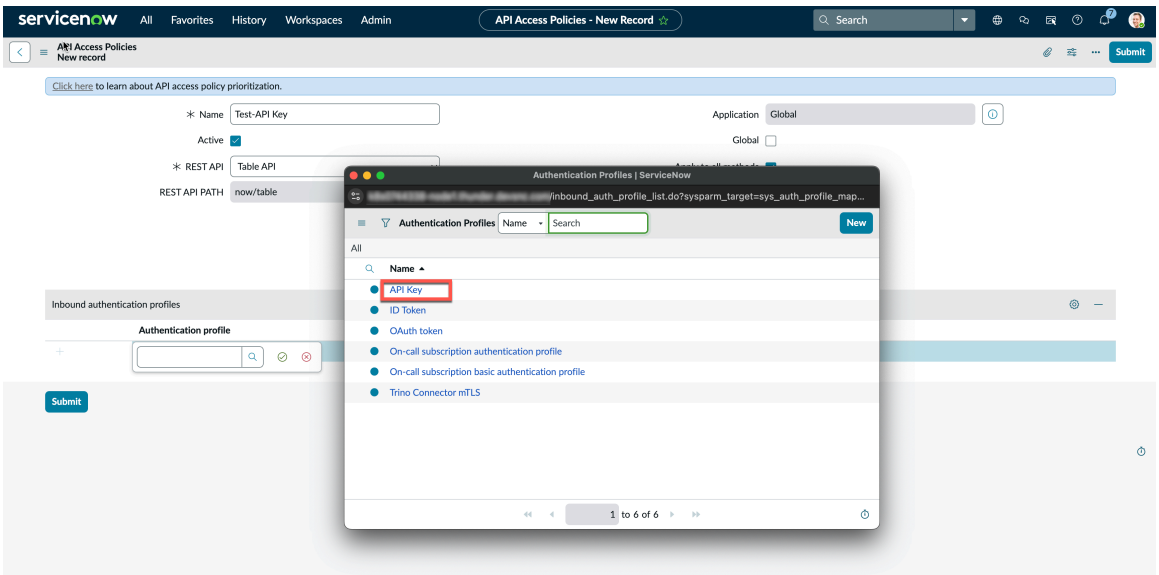
Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès API.
Actif	Option pour rendre la politique d'accès API active.
API REST	API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'API de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.
Méthode HTTP	Méthode utilisée pour interagir avec l'API. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une API REST, vous devez créer des politiques individuelles pour chaque version.
Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez ce champ pour appliquer la politique d'authentification à toutes les méthodes, versions et ressources de l'API. **Remarque :** L'authentification basée sur le jeton n'est pas autorisée dans la politique API REST globale.
Appliquer à toutes les méthodes	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les méthodes, versions et ressources de l'API.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Appliquer à toutes les ressources	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les ressources.



d. Ajoutez le profil d'authentification API qui a été créé.

e. Envoyez le formulaire.

Vous pouvez envoyer l'appel d'API REST avec le x-sn-apikey (jeton) qui a été généré par lors ServiceNow AI Platform de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration d'authentification.

> **⚠ Avertissement :**
> Utilisez la demande **POST** lors de la soumission d'informations sensibles au serveur.

Configurer HMAC : authentification basée sur un jeton

Configurez HMAC pour prendre en charge l'authentification pour les points de terminaison d'API REST.

Avant de commencer

Rôle requis : admin

Module d'extension requis : clé API et authentification HMAC (com.glide.tokenbased_auth)

Procédure

1. Créez une configuration HMAC.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Configuration HMAC**.

b. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez également utiliser **l'encodage HMAC SHA256 Base64 par défaut** créé lors de l'installation du plugin.

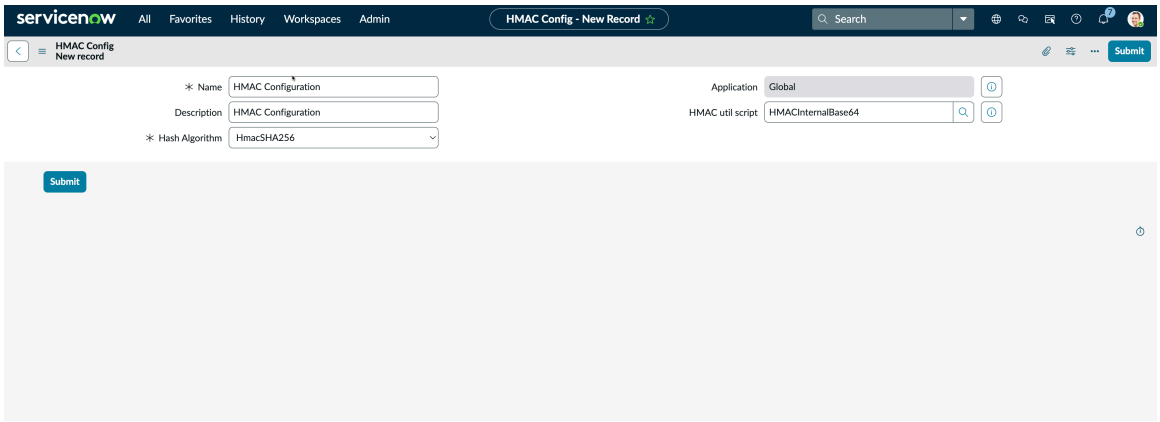
c. Renseignez les champs du formulaire :

Configuration HMAC

Champ	Description
Nom	Nom de la configuration HMAC.
Application	Périmètre de la configuration.
Description	Description détaillée de la configuration.
Algorithme de hachage	Choisissez l'algorithme de hachage. Options disponibles : ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
Script d'utilitaire HMAC	Script utilitaire pour HMAC. **Remarque :** Si vous validez l'authentification HMAC à l'aide du corps de la demande, de l'horodatage et du secret sans ID de clé, procédez comme suit : ▪ Créer un include de script personnalisé en tant que script d'utilitaire HMAC ▪ Utilisez cet utilitaire d'include de script pour interpréter l'horodatage transmis et le corps de la demande. Pour chaque secret partagé créé dans l'instance ServiceNow® , il existe un ID de clé. Vous devez configurer l'ID de clé dans l'ID de clé par défaut dans le profil d'authentification HMAC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



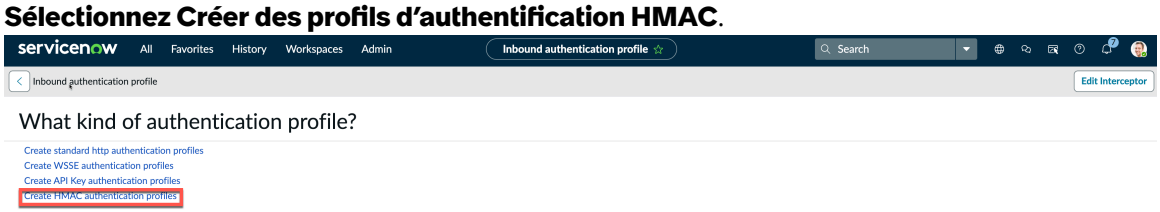
d. Envoyez l'enregistrement.

2. Créez un profil d’authentification entrant.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Profils d’authentification entrants**.

b. Sélectionnez **Nouveau**.
Le système affiche le message Quel type de profil d’authentification ?

c. Sélectionnez Créer des profils d’authentification HMAC.



d. Remplissez les champs du formulaire.

Profils d’authentification HMAC

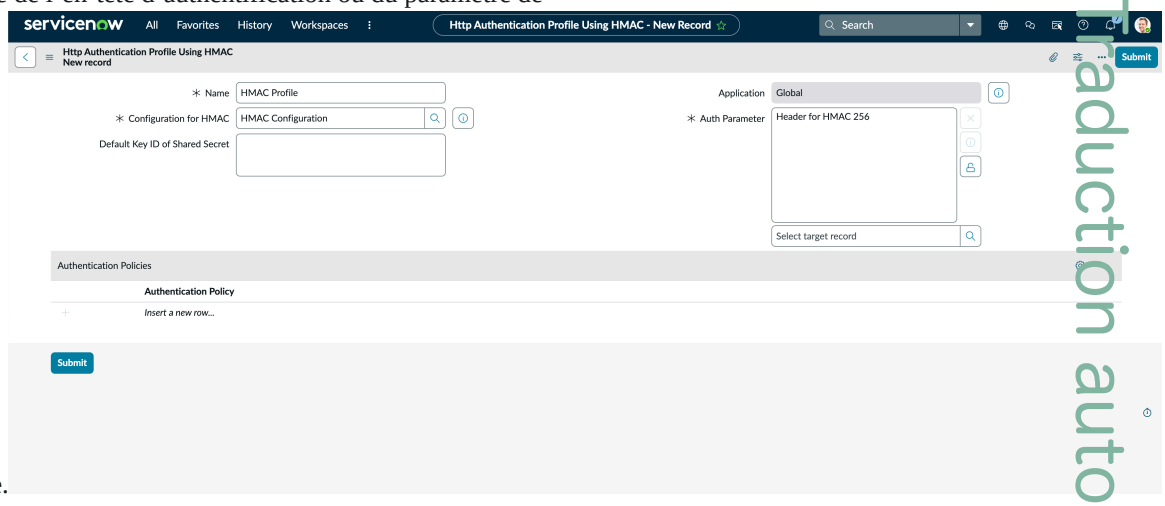
Champ	Description
Nom	Nom permettant d’identifier la politique d’authentification.
Application	Périmètre de la politique d’authentification.
Configuration pour HMAC	Sélectionnez la configuration HMAC qui a été créée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Paramètre d'authentification	Sélectionnez le paramètre d’authentification de la demande d’authentification. Vous pouvez sélectionner les options par défaut ou créer un nouveau paramètre d’authentification : ▪ x-sn-hmac-signature-256 : en-tête d’authentification ▪ x-sn-hmac-signature-256 : paramètre de requête
ID de clé par défaut du secret partagé	Les informations de jeton qui peuvent être mises à jour dans ce champ pour l’utilisation de HMAC.

Remarque :
L’option sélectionnée doit être définie dans l’appel REST dans le cadre de l’en-tête d’authentification ou du paramètre de requête.



e. Envoyez le formulaire.

3. Créez un secret HMAC.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Secret HMAC de l'API REST**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire :

Secret HMAC de l'API REST

Champ	Description
Nom	Nom permettant d’identifier le secret HMAC de l’API REST.
Description	Description du secret HMAC de l’API REST.
Actif	État du secret HMAC de l’API REST.

Traduction automatique

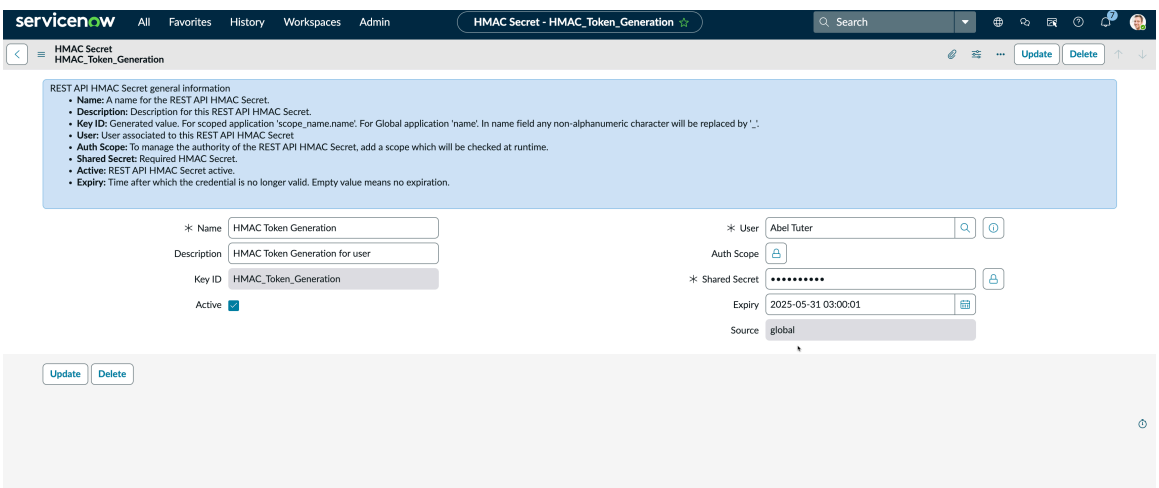
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utilisateur	Utilisateur associé au secret HMAC de l'API REST. Utilisez l'icône de recherche pour sélectionner l'utilisateur.
ID clé	ID clé qui doit être envoyé dans le cadre de l'appel REST. L'ID de clé est généré après avoir soumis le formulaire.
Secret partagé	Secrets partagés de l'utilisateur. Par exemple, le mot de passe.
Source	Source de l'enregistrement.
Expiration	Heure après laquelle les informations d'identification ne sont plus valides. Une valeur vide signifie qu'il n'y a pas d'expiration. **Remarque :** Pour plus d'informations sur l'expiration du jeton, reportez-vous à la section Nettoyage de l'expiration du jeton .

d. Envoyez le formulaire.

e. Ouvrez l'enregistrement qui a été créé.

Recherchez l'ID de clé généré par le ServiceNow AI Platform pour l'utilisateur.



Remarque : Vous pouvez ajouter l'ID de clé généré pendant l'ID de clé dans le profil d'authentification créé pour HMAC si vous ne souhaitez pas spécifier le paramètre d'authentification ou de requête pour l'appel d'API.

4. Créez une politique d'accès REST API.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.

b. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Remplissez les champs du formulaire.

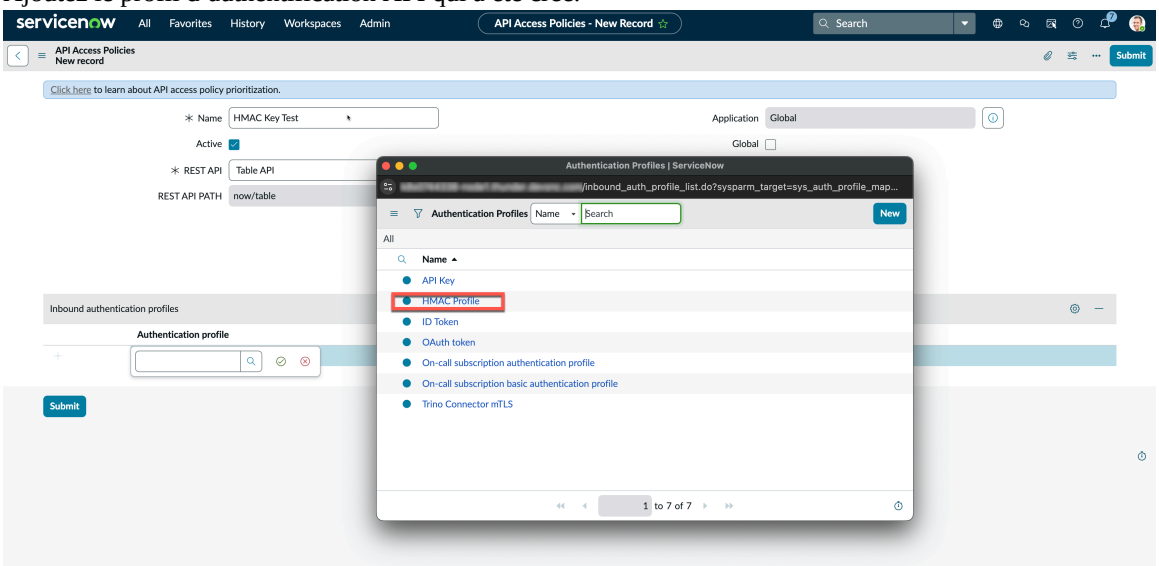
Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès API.
Actif	Option pour rendre la politique d'accès API active.
API REST	API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'API de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.
Méthode HTTP	Méthode utilisée pour interagir avec l'API. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une API REST, vous devez créer des politiques individuelles pour chaque version.
Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez ce champ pour appliquer la politique d'authentification à toutes les méthodes, versions et ressources de l'API. **Remarque :** L'authentification basée sur le jeton n'est pas autorisée dans la politique API REST globale.
Appliquer à toutes les méthodes	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les méthodes, versions et ressources de l'API.
Appliquer à toutes les ressources	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les ressources.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Ajoutez le profil d'authentification API qui a été créé.



e. Envoyez le formulaire.
Vous pouvez envoyer l'appel d'API REST :

- Avec la signature x-sn-hmac-signature-256 qui a été générée lors ServiceNow® de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration d'authentification.
- Avec un script de pré-demande avec un secret partagé spécifié dans le cadre de la demande.

> ⚠ **Avertissement :**
> Utilisez la demande **POST** lors de la soumission d'informations sensibles au serveur.

Nettoyage de l'expiration du jeton

Détails sur la façon de nettoyer l'expiration du jeton à l'aide de différentes propriétés système.

Une fois la clé API ou le secret HMAC expiré, les détails sont conservés pendant 7 jours. Une tâche planifiée Nettoyer les informations d'identification d'authentification de jeton expirées supprime ensuite les clés API ou les secrets HMAC ayant expiré. Vous pouvez configurer ce comportement et contrôler la suppression à l'aide des propriétés suivantes :

- **com.snc.platform.security.token.auth.cleanup** : utilisez cette propriété si vous souhaitez supprimer des clés API et des jetons HMAC expirés. Par défaut : vrai.
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver le jeton d'API expiré dans le système. Par défaut 7.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver le jeton HMAC expiré dans le système. Par défaut 7.

Pour accéder à la propriété d'expiration du jeton, saisissez sys_properties.list dans la barre de navigation, puis recherchez les propriétés suivantes. Modifiez la date de péremption en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique d'accès API

La politique d'accès API définit les autorisations et la durée d'accès à une API.

La politique d'accès API vous permet de restreindre l'accès aux API entrantes ServiceNow® en fonction du type d'authentification et des critères de filtre spécifiés dans la politique d'accès.

Voici la prise en charge de la politique d'authentification à trois niveaux pour les sessions non interactives :

- **API REST** : l'administrateur peut définir une politique d'authentification API globale ou une politique d'authentification spécifique à l'API.
- **API SOAP** : l'administrateur peut définir une politique d'authentification API globale ou une politique d'authentification spécifique à l'API.
- **Processeur système/d'exportation** : l'administrateur peut définir cinq profils d'authentification du système de base, qui peuvent être utilisés pour appliquer un profil d'authentification à une politique d'authentification API ou à une politique d'authentification spécifique au processeur.

Remarque :
Si vous ajoutez une stratégie d'authentification globale, elle s'applique à toutes les API REST, API SOAP ou processeurs système/d'exportation.

Voici les modules d'extension installés automatiquement pour les politiques d'API et le périmètre d'authentification :

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

Vous pouvez configurer la politique de blocage globale par défaut ou créer une politique d'accès API personnalisée en fonction de vos besoins de sécurité. Et appliquez des critères de filtre qui contiennent des conditions de filtre ou des requêtes qui sont utilisées comme entrées de politique pour une politique d'authentification.

Les politiques d'accès API suivantes sont prises en charge dans ServiceNow®:

- Politiques d'accès REST API
- Politiques d'accès de l'API SOAP

Pour plus d'informations sur les stratégies relatives aux processeurs d'exportation, reportez-vous à la section Politique d'accès pour le système ou les processeurs d'exportation.

Politiques d'accès REST API

Les politiques d'accès des API REST vous permettent de restreindre l'accès aux API REST entrantes en fonction du type d'authentification et des critères de filtre spécifiés dans la politique d'accès.

Une API REST, également connue sous le nom d'API RESTful, est un type d'interface de programmation d'application (API) qui adhère aux directives du style architectural REST. Les API REST offrent un haut degré de flexibilité, ce qui les rend répandues sur le Web.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les critères de filtre contiennent des conditions de filtre ou des requêtes qui sont utilisées comme entrées de politique pour une politique d'authentification.

Vous pouvez configurer la politique de blocage globale par défaut ou créer une politique d'accès API personnalisée en fonction de vos besoins de sécurité. Par exemple, vous pouvez créer une politique d'accès API personnalisée qui autorise uniquement le type d'authentification OAuth 2.0 à partir d'une plage spécifiée d'adresses IP. Les demandes d'authentification d'autres types d'authentification et les demandes d'accès à partir d'adresses IP autres que les adresses IP spécifiées sont refusées.

Activer la politique d'accès REST API

Vous pouvez activer le module d'extension Politique d'accès de l'API REST (com.glide.rest.policy) si vous disposez du rôle administrateur. L'application inclut des données de démonstration et installe les applications et modules d'extension ServiceNow® Store connexes s'ils ne sont pas déjà installés.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les éléments suivants sont installés avec la politique d'accès REST API :

- Modules d'extension : com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tables : sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

Pour plus d'informations, consultez Authentification adaptative.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Politique d'accès de l'API REST (com.glide.rest.policy) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Créer un profil d'authentification

Créez un profil d'authentification et ajoutez-y une ou plusieurs politiques d'authentification. Vous pouvez également configurer les profils **d'authentification de jeton d'ID** et **de jeton OAuth** qui sont disponibles par défaut.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez appliquer des stratégies d'authentification, de plage IP, basées sur les rôles, basées sur l'utilisateur, etc. avec l'authentification réciproque et l'authentification personnalisée.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.
2. Sélectionnez **Nouveau**.
   Le système affiche le message. Quel type de profil d'authentification ?
3. Sélectionnez **Créer des profils d'authentification HTTP standard**.
4. Remplissez les champs du formulaire.

Formulaire de profil d'authentification standard

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Description	Description de la politique d'authentification.
Actif	Option pour rendre la politique d'authentification active.
Application	Périmètre de la politique d'authentification.
Type	Type d'authentification disponible. Vous pouvez sélectionner **Authentification de base**, **Jeton d'ID**, **Authentification basée sur certificat** ou **OAuth**.
Entité OAuth	Profil de l'entité OAuth. Ce champ apparaît uniquement lorsque le **jeton d'ID** ou **OAuth** est sélectionné dans **Type**.

5. Double-cliquez sur **Insérer une nouvelle ligne**.
6. Sélectionnez une politique d'authentification dans la liste et sélectionnez .

Remarque :
Ne sélectionnez pas Politique d'accès autorisée ou Politique d'accès refusée. Ces politiques ne sont destinées qu'aux connexions des utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

Remarque :

En-tête Authentifier [www-authentifier].

Lorsque la politique d'accès REST API est active, nous rappelons le profil d'authentification mappé le plus récemment dans l'en-tête d'authentification. Si vous souhaitez que le serveur renvoie tous les schémas d'authentification, utilisez la propriété glide.security.response.authenticate.header.auth_profile.first_scheme_only et définissez-la sur **false**. La réponse est renvoyée avec plusieurs en-têtes. Par exemple :

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Créer une politique d'accès REST API

Créez une politique d'accès API et mappez un profil d'authentification pour restreindre le type d'authentification d'une REST API. Par exemple, vous pouvez créer une politique d'accès API qui autorise uniquement l'authentification par jeton d'ID pour une API REST.

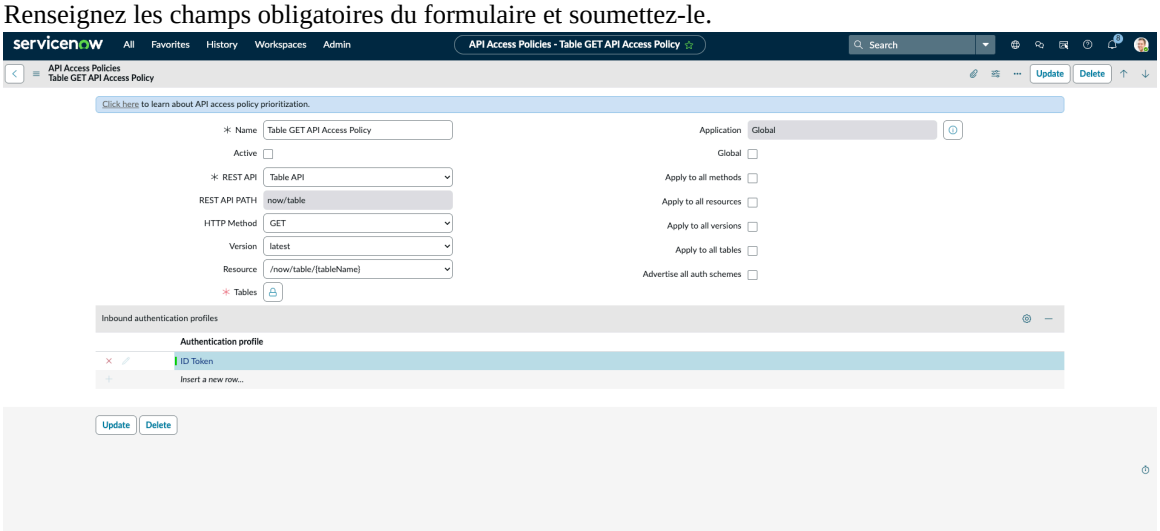
Avant de commencer

Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, voir Créer un profil d'authentification.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs obligatoires du formulaire et soumettez-le.



Remarque :

Vous devez rouvrir le formulaire soumis pour renseigner les champs supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d’accès API.
Actif	Option pour rendre la politique d’accès API active.
API REST	API REST à laquelle la politique d’accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d’API de l’API REST. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Par exemple, **now/attachment**.
Méthode HTTP	Méthode utilisée pour interagir avec l’API. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d’authentification pour toutes les versions d’une API REST, vous devez créer des politiques individuelles pour chaque version.
Ressource	Ressource enfant de l’API REST. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Par exemple, **/now/attachment**
Table	Tables auxquelles la politique d’accès API s’applique. Cette option s’applique uniquement aux politiques de l’API `Table` .
Application	Périmètre de l'application.
Global	Option permettant d’appliquer la politique à toutes les méthodes, versions et ressources de l’API.
Appliquer à toutes les méthodes	Option permettant d’appliquer la politique à toutes les méthodes, versions et ressources de l’API.
Appliquer à toutes les ressources	Option permettant d’appliquer la politique à toutes les ressources d’API ou à toutes les ressources d’API.
Appliquer à toutes les versions	Option permettant d’appliquer la politique à toutes les versions de l’API ou aux versions de l’API.
Appliquer à toutes les tables	Option permettant d’appliquer la politique à toutes les tables. Cette option s’applique uniquement aux politiques de l’API `Table` .
R : Publier tous les schémas d’authentification	Détermine si l’en-tête `WWW-Authenticate` inclut tous les schémas d’authentification configurés. Lorsqu’il est défini sur `faux` (valeur

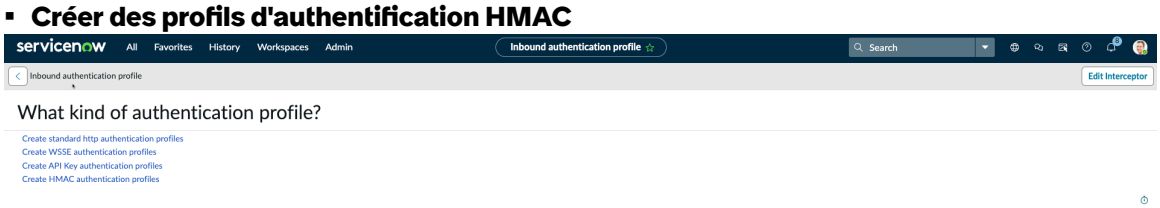
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	par défaut), l'en-tête inclut uniquement le profil d'authentification le plus récemment configuré dans la politique. Quand la valeur est définie sur `vrai`, l'en-tête répertorie tous les schémas d'authentification configurés.

Remarque :
Pour en savoir plus sur la hiérarchisation de la politique d'accès API, reportez-vous à la section Accès API : ordre de priorité de la politique.

4. Double-cliquez sur **Insérer une nouvelle ligne**.
5. Sélectionnez un profil d'authentification entrant dans la liste et sélectionnez .
   Par exemple, vous pouvez ajouter **une authentification de base**, **un jeton d'ID**, **une authentification basée sur un certificat**, **une authentification OAuth** ou **WSSE**.
   a. Pour ajouter un ou plusieurs profils d'authentification entrants, sélectionnez **Nouveau** pour créer un nouveau profil.
   b. **Choisir quel type de profils d'authentification ?**
      - **Créer des profils d'authentification http standard**
      - **Créer des profils d'authentification WSSE**
      - **Créer des profils d'authentification de clé API**
      - **Créer des profils d'authentification HMAC**



   c. Après avoir créé le profil d'authentification, enregistrez l'enregistrement.
6. Sélectionnez **Soumettre** pour soumettre la politique d'accès à l'API REST.

Accès API : ordre de priorité de la politique

Découvrez la logique de hiérarchisation des politiques si plusieurs politiques d'accès API sont configurées pour votre ServiceNow® instance.

Les politiques d'accès API sont classées par ordre de priorité en fonction du type de politique d'API REST défini sur votre ServiceNow® instance.

L'approche consiste à définir différents poids pour chaque partie de l'API (méthode, ressource et version).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La politique d'API est priorisée pour les modèles non globaux d'abord, puis pour les paramètres globaux. En d'autres termes, une politique d'accès non globale remplacera toujours une politique d'accès API globale.

Les logiques de hiérarchisation sont les suivantes :

Ordre de priorité

Champs	Priorité	Logique de hiérarchisation
Méthode, ressource et version	1	Si les 3 champs correspondent à la politique, cette politique prend la 1ère priorité.
Ressource Method+	2	Si les 2 champs correspondent à la politique, cette politique prend la 1ère priorité.
Ressource + version	3	Si les 2 champs ainsi que le champ **Appliquer à toutes les méthodes correspondent à** la politique, cette politique prend la 3e priorité.
Ressource	4	Si le champ et le champ **Appliquer à toutes les méthodes correspondent à** la politique, cette politique prend la 4e priorité.
Méthode + version	5	Si les 2 champs ainsi que le champ **Appliquer à toutes les ressources** correspondent à la politique, cette politique prend la 5e priorité.
Fonction de message REST	6	Si le champ et le champ **Appliquer à toutes les ressources correspondent à** la politique, cette politique prend la 5e priorité.
Version	7	Si le champ et les champs **Appliquer à toutes les méthodes** et **Appliquer à toutes les versions** correspondent à la politique, cette politique prend la 7e priorité.
Global et Appliquer à toutes les méthodes	8	Si les champs **Global** est `vrai` et **Appliquer à toutes les méthodes** est `faux` , cette politique prend la 8e priorité.
Global et Appliquer à toutes les méthodes	9	Si les champs **Global** ont la valeur `vrai` et **Appliquer à toutes les méthodes** a la valeur `vrai`, cette politique prend la 9e priorité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Périmètre d'authentification REST API

Utiliser le périmètre d'authentification de l'API REST pour fournir l'accès à une API REST spécifique

Auparavant, chaque jeton d'accès ou jeton OIDC était lié au périmètre du compte utilisateur qui dispose d'un accès complet aux API REST de l'utilisateur. Dès Yokohama la publication, pour fournir un accès uniquement aux API REST particulières, le **périmètre d'authentification de l'API REST** est introduit.

Après avoir créé l'enregistrement du périmètre d'authentification de l'API REST, pour accéder à cette API REST, vous devez associer le même périmètre d'authentification à l'entité OAuth qui doit avoir accès à cette API REST. Pour une nouvelle entité OAuth, le périmètre d'authentification par défaut est vide.

Remarque :
À moins que vous ne disposiez d'un enregistrement de périmètre d'authentification de l'API REST, l'API REST est accessible par n'importe quelle entité OAuth valide.

Vous devez lier manuellement le périmètre d'authentification à l'entité OAuth. Le compte d'utilisateur est un périmètre spécial. S'il est associé à une entité OAuth, il peut accéder à n'importe quelle API même si vous avez créé un enregistrement de périmètre d'authentification de REST API avec un périmètre d'authentification différent.

Pour en savoir plus sur l'utilisation du périmètre d'authentification de l'API dans la nouvelle expérience d'intégration entrante, consultez Intégrations entrantes.

Remarque :

- Une fois que le périmètre d'authentification de l'API REST est activé et ajouté au périmètre d'authentification de l'API REST, tous les jetons OAuth existants ne peuvent plus accéder à cette API, à moins que l'administrateur n'ajoute ce périmètre d'authentification à l'entité OAuth correspondante
- L'administrateur est chargé de s'assurer que le oauth_entity dispose du périmètre d'authentification approprié après avoir lié le périmètre d'authentification à l'API REST.
- Les jetons d'accès OAuth émis par ServiceNow prennent en charge le périmètre d'authentification.
- Le jeton OIDC qui n'est pas émis par ServiceNow est validé par ServiceNow.
- Le jeton OIDC a son champ d'application à partir de l'IDP lorsque vous avez besoin d'un jeton d'ID. Ici, le périmètre d'authentification est pour ServiceNow et non pour tiers (IdP).

Configurations pour le périmètre de REST API

Pour configurer le périmètre de l'API REST, procédez comme suit :

- Créer un périmètre d'authentification
- Lier le périmètre d'authentification à l'API REST
- Lier le périmètre d'authentification à l'entité OAuth
- Effectuer un flux OAuth pour obtenir un jeton d'accès OAuth
- Utiliser le jeton d'accès OAuth pour effectuer l'appel d'API

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer le périmètre d'authentification de l'API REST

Vous pouvez activer le module d'extension Champ d'application d'authentification de l'API REST (com.glide.rest.auth.scope) pour lier l'entité OAuth à des champs d'application d'authentification.

Avant de commencer
Installez les modules d'extension suivants :

- OAuth 2.0
- Fournisseur d'API REST
- Périmètre d'authentification
- Périmètre de REST API

Remarque :
Le *REST API Scope* module d'extension est ajouté dans le cadre de la Tokyo version.

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Champ d'application d'authentification de l'API REST (*com.glide.rest.auth.scope*) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Périmètre d'authentification de l'API REST Propriétés et tables

Le module d'extension Champ d'application d'authentification de l'API REST (com.glide.rest.auth.scope) inclut les propriétés, tables et scripts système suivants.

Propriétés du périmètre d'authentification de l'API REST

Le périmètre d'authentification de l'API REST ajoute les propriétés système suivantes.

Propriétés

Nom	Description
com.glide.rest.api.auth.scope.check.enable	Cette propriété permet de désactiver la vérification du périmètre d'authentification au niveau de la plateforme.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
	Si la valeur est définie sur faux, pendant l'exécution, la vérification du périmètre d'authentification est ignorée, qu'elle soit liée ou non à l'API REST. Par défaut, cette propriété est définie sur vrai. Cette propriété est utilisée lorsque vous souhaitez revenir au comportement de la version précédente.
`com.glide.oauth.token.scope.useraccount`	Cette propriété n'est utilisée que lorsque le `useraccount` périmètre d'authentification est supprimé et rajouté manuellement par l'utilisateur final. Dans ce cas, l'ID système de est `useraccount` modifié. Il est nécessaire de mettre à jour cette propriété vers la nouvelle sys_id. Pendant l'exécution, l'ID système du périmètre d'authentification est utilisé à la place du nom du périmètre d'authentification.

Tables des périmètres d'authentification de l'API REST

Champ d'application d'authentification de l'API REST les tables suivantes.

Tables

Nom	Description
Périmètre d'authentification (sys_auth_scope)	Cette table définit le périmètre d'authentification qui peut être lié à l'API REST et à l'entité OAuth. Le nom du champ d'application d'authentification doit être unique et global.
Périmètre d'authentification de REST API (sys_api_access_scope)	Cette table relie l'API REST au périmètre d'authentification.

Configurer le périmètre d'authentification de l'API REST

Liez l'entité OAuth à un périmètre d'authentification pour gérer le jeton afin d'accéder aux API REST qui sont liées au périmètre d'authentification.

Avant de commencer
Installez les modules d'extension suivants :

- OAuth 2.0
- Fournisseur d'API REST

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Périmètre d’authentification
- Périmètre d'authentification REST API

Remarque :
Le *REST API Auth Scope* module d’extension est ajouté dans le cadre de la Tokyo version.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Périmètres d'authentification API** > **Périmètre d'authentification REST API**.
   La page Périmètres d’authentification de l’API REST s’affiche.
2. Pour configurer un nouveau périmètre d’authentification de l’API REST, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Périmètre d'authentification REST API

Nom	Nom unique qui identifie le périmètre d’authentification de l’API REST.
Actif	Cochez cette case pour activer la configuration.
Application	Champ d'application de l'application en lecture seule.
API REST	API REST à laquelle le périmètre d’authentification est appliqué. Par exemple, l’API Table.
Périmètre d'authentification	Sélectionnez le périmètre d’authentification à partir de l’icône de recherche.
CHEMIN REST API	Chemin d’API de l’API REST. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Par exemple, now/table.
Méthode HTTP	Méthode utilisée pour interagir avec l’API. Sélectionnez la méthode dans la liste déroulante. Vous pouvez désactiver manuellement l’option **Appliquer le périmètre d’authentification à toutes les méthodes HTTP dans le champ de cette API** du formulaire pour sélectionner la méthode.
Version de REST API	Version de l'API. Par exemple, v1. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Vous pouvez désactiver manuellement l’option **Appliquer le périmètre d’authentification à toutes les versions dans ce champ d’API du** formulaire pour sélectionner la version.

Traduction automatique

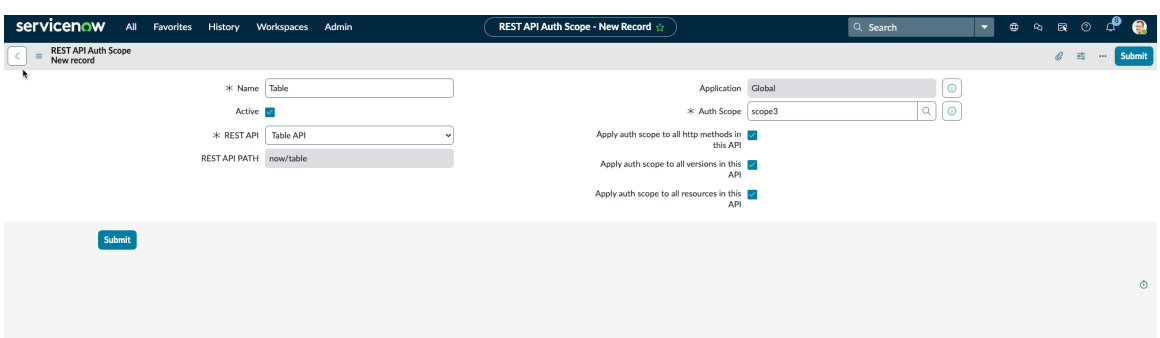
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, /now/table. Vous pouvez désactiver manuellement **l'option Appliquer le périmètre d'authentification à toutes les ressources dans ce champ API** du formulaire pour sélectionner les ressources.
Appliquer le périmètre d'authentification à toutes les méthodes HTTP dans cette API.	Lorsqu'elle est activée, elle applique le périmètre d'authentification à toutes les méthodes HTTP dans l'API.
Appliquer le périmètre d'authentification à toutes les versions dans cette API.	Lorsque cette option est activée, elle applique le périmètre d'authentification à toutes les versions de l'API.
Appliquer le périmètre d'authentification à toutes les ressources dans cette API.	Lorsque cette option est activée, elle applique le périmètre d'authentification à toutes les ressources de l'API

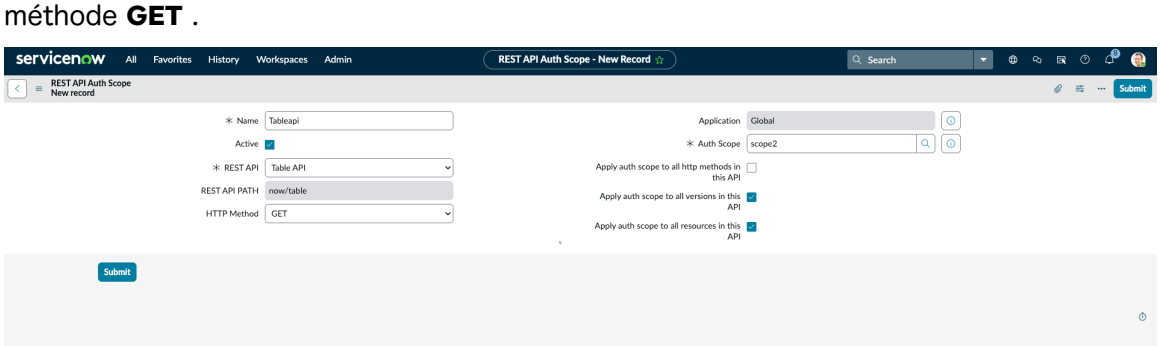
4. Cliquez sur **Envoyer**.
   En fonction de l'API REST et du périmètre d'authentification sélectionnés, les API récupèrent les informations spécifiques au périmètre.

Example: Envisagez de créer trois périmètres d'authentification de l'API REST pour l'API de table

Le périmètre de la première authentification est mappé à **l'API de table** avec toutes les méthodes, versions et ressources HTTP activées.



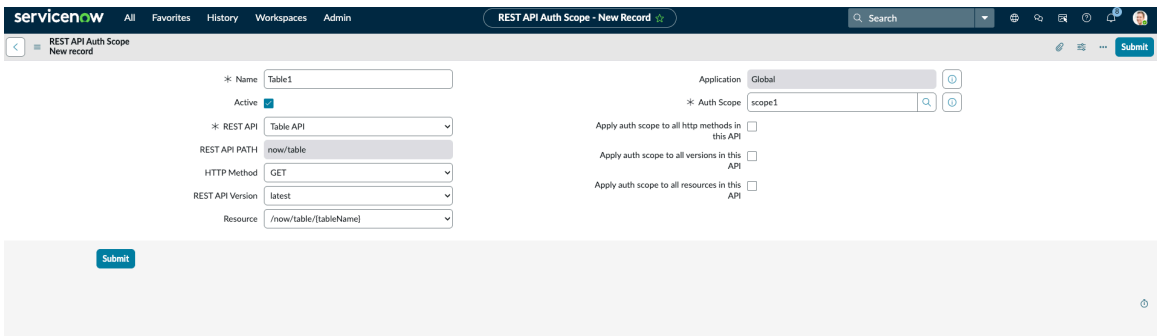
Le deuxième périmètre d'authentification est mappé à **l'API de table** avec toutes les versions et ressources activées. Mais, vous choisissez la méthode HTTP, dans cet exemple, la méthode **GET** .



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le troisième périmètre d'authentification est mappé à **l'API de table** sans les méthodes, versions et ressources HTTP activées. Cependant, vous choisissez manuellement la méthode, la version et la ressource HTTP. Dans cet exemple, la méthode HTTP est **GET**, la version de l'API REST est **la dernière** et la ressource est `/now/table/{tableName}`.



Si tous ces champs d'application d'authentification sont créés, vous pouvez utiliser la méthode **GET** avec les trois champs d'application, mais pour les méthodes **POST,PUT**, **DELETE** ou **PATCH** , seul **le champ d'application 3** peut être utilisé.

Dépannage du périmètre de l'API REST

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de la configuration ou de l'exécution du périmètre de l'API REST.

Dépannage

Problème	Action
L'API REST est liée au périmètre d'authentification, mais en cours d'exécution, il n'y a pas de vérification du périmètre d'authentification, même à l'aide de l'authentification par jeton de porteur.	• Assurez-vous que l'enregistrement sys_api_access_policy est actif. L'exécution ignore les enregistrements inactifs. • Vérifiez si la propriété *`com.glide.rest.api.auth.scope.check.enable`* est définie sur faux. • Vérifiez si le jeton OAuth a un périmètre d'authentification de compte utilisateur .
L'API REST est liée à *`auth_scope1`*, mais le jeton d'accès qui a *`auth_scope2`* est également capable d'y accéder.	• Vérifiez si cet enregistrement est actif. • Vérifiez ce REST, vérifiez si d'autres enregistrements, qui ont les mêmes API, mais différentes appliquent des méthodes, des versions ou des ressources.
L'API REST est liée au périmètre d'authentification, mais en cours d'exécution, il n'y a pas de vérification du périmètre d'authentification pour *`basicAuth`* et *`mutualAuth`*.	C'est normal car le périmètre d'authentification de l'API REST ne s'applique qu'au jeton d'accès OAuth ou au jeton OIDC. Elle n'applique pas BasicAuth, les cookies de session et l'authentification basée sur certificat.
L'appel de l'API REST renvoie 403 lors de l'utilisation du jeton d'accès OAuth.	Vérifiez le message d'erreur « Périmètre d'accès à l'API requis manquant ». Si elle est trouvée, la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Problème	Action
	vérification du champ d'application d'authentification échoue pour cette API REST
Le compte d'utilisateur prédéfini est supprimé et la restauration n'est pas sûre.	Exporter useraccount au format xml depuis l'autre instance et l'importer ou créer un useraccount et modifier la propriété `glide.oauth.token.scope.useraccount` système dans l'enregistrement sys_id nouvellement créé.

Forum Aux Questions

Voici quelques-unes des questions fréquemment posées lors de l'utilisation du périmètre d'authentification de l'API REST :

Un jeton OAuth peut-il être lié à plusieurs périmètres d'authentification ?

Oui, un oauth_entity peut être lié à plusieurs champs d'application d'authentification, tous les jetons OAuth émis par cet oauth_entity ont les mêmes champs d'application d'authentification.

Différents jetons OAuth avec différents champs d'application d'authentification peuvent-ils accéder à la même API REST ?

Oui, pour une même API REST, différents périmètres d'authentification peuvent y accéder. Tant qu'un périmètre d'authentification est mis en correspondance, il renvoie les résultats.

Le jeton d'accès OAuth avec le périmètre d'authentification du compte utilisateur **peut-il accéder à toutes les API REST ?**

Oui, le compte utilisateur dispose d'un accès complet au périmètre d'authentification.

Le périmètre OAuth du jeton d'accès OAuth peut-il être modifié dynamiquement ?

Oui, l'authentification incluse dans le périmètre n'est pas codée en dur avec le jeton d'accès dans la table oauth_credential . Au lieu de cela, le périmètre d'authentification est obtenu à partir des oauth_entity liés pendant l'exécution.

Le jeton OAuth peut-il conserver les mêmes champs d'application d'authentification après l'actualisation ?

Oui, le périmètre d'authentification ne changera pas après l'actualisation du jeton, sauf si oauth_admin modifiez le périmètre d'authentification lié à oauth_entity.

L'enregistrement du champ d'application d'authentification du compte d'utilisateur **prédéfini est supprimé. Un nouveau champ d'application d'authentification portant le nom** useraccount **peut-il être créé ?**

La création d'un nouveau champ d'application d'authentification avec le même compte d'utilisateur ne fonctionne pas. Dans l'exécution, il utilise le sys_id au lieu du nom pour effectuer la vérification du périmètre d'authentification et modifier la propriété `glide.oauth.token.scope.useraccount` système sur l'enregistrement de sys_id nouvellement créé.

Si l'administrateur modifie l'authentification incluse dans le périmètre lié à oauth_entity**, tous les jetons d'accès OAuth existants émis par cette entité OAuth sont-ils également changés ?**

Oui, le périmètre d'authentification n'est pas directement lié au jeton d'accès OAuth qu'il reçoit de oauth_entity pendant l'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Différents jetons d'accès OAuth émis par le même `oauth_entity` peuvent-ils avoir des champs d'application d'authentification différents ?

Non, tous les accès au jeton sont émis par le même `oauth_entity` et ont toujours les mêmes champs d'application d'authentification.

Un utilisateur peut-il définir différents champs d'application d'authentification pour un point de terminaison particulier ?

Non, il existe une vérification de contrainte unique pour un point de terminaison d'API REST particulier. Toutefois, pour un même point de terminaison d'API REST, il peut avoir plusieurs périmètres d'authentification correspondants.

La vérification du champ d'application d'authentification est-elle également utilisée pour BasicAuth ?

Non, la vérification du champ d'application d'authentification est uniquement un jeton d'accès OAuth et un jeton OIDC, elle n'est pas demandée *`basicAuth`* et *`mutualAuth`*

Politiques d'accès de l'API SOAP

Les politiques d'accès de l'API SOAP vous permettent de restreindre l'accès aux API SOAP entrantes en fonction du type d'authentification et des critères de filtre spécifiés de la politique d'accès.

Les politiques d'accès de l'API SOAP vous permettent d'appliquer le profil d'authentification entrant et les politiques d'accès de l'API au SOAP entrant et aux API SOAP scriptées.

Vous pouvez tirer parti ServiceNow des politiques d'accès d'API telles que la plage d'adresses IP et les restrictions basées sur les rôles pour autoriser ou interdire les appels d'API SOAP entrants en fonction de l'authentification.

En tant qu'administrateur, vous pouvez effectuer les actions suivantes pour appliquer les politiques.

- Activez les modules d'extension Politique d'accès et Profil d'authentification de l'API SOAP. Pour plus d'informations, consultez Activer la politique d'accès de l'API SOAP.
- Créez des politiques d'accès de l'API SOAP et associez ces politiques à un profil d'authentification. Pour plus d'informations, consultez Créer une politique d'accès de l'API SOAP et Créer un profil d'authentification.

  Remarque :
  Les politiques s'appliquent à l'API de table SOAP ou à l'API SOAP scriptée. Outre le profil d'authentification http et WSSE standard.

- Créez des politiques d'authentification telles que des plages IP et des restrictions basées sur les rôles, et associez cette politique au profil d'authentification. Pour plus d'informations, consultez Créer une politique d'authentification API.

Activer la politique d'accès de l'API SOAP

Pour la politique d'accès de l'API SOAP, installez le module d'extension Politique d'accès de l'API SOAP (com.glide.soap.policy).

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'élément suivant est installé avec le module d'extension Politique d'accès de l'API SOAP : Processor Access Policy (com.glide.processor.policy)

Module d'extension dépendant : Authentication Profile (com.glide.auth.profile)

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension SOAP API Access Policy (com.glide.soap.policy) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Créer un profil d'authentification

Créez un profil d'authentification et ajoutez-y une ou plusieurs politiques d'authentification. Vous pouvez également configurer les profils **d'authentification de jeton d'ID** et **de jeton OAuth** qui sont disponibles par défaut.

Avant de commencer

Rôle requis : admin

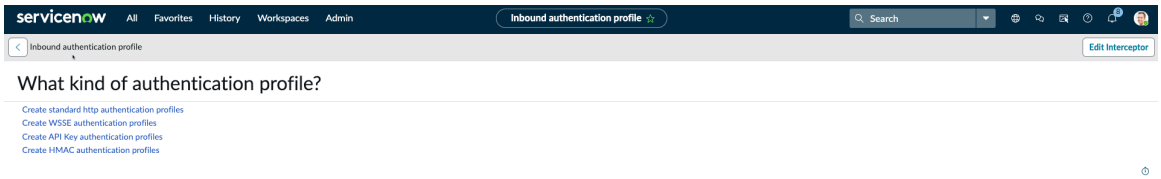
Remarque :
Vous pouvez appliquer des stratégies d'authentification, de plage IP, basées sur les rôles, basées sur l'utilisateur, etc. avec l'authentification réciproque et l'authentification personnalisée.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.
2. Sélectionnez **Nouveau**.
   Le système affiche le message. Quel type de profil d'authentification ?
3. **Choisir quel type de profils d'authentification ?**
   - **Créer des profils d'authentification http standard**
   - **Créer des profils d'authentification WSSE**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Remplissez les champs du formulaire.

Formulaire de profil d'authentification standard

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Description	Description de la politique d'authentification.
Actif	Option pour rendre la politique d'authentification active.
Application	Périmètre de la politique d'authentification.
Type	Type d'authentification disponible. Vous pouvez sélectionner **Authentification de base**, **Jeton d'ID**, **Authentification basée sur un certificat**, **OAuth** ou **WSSE** (dans le cas d'un profil d'authentification WSE).
Entité OAuth	Profil de l'entité OAuth. Ce champ apparaît uniquement lorsque le **jeton d'ID** ou **OAuth** est sélectionné dans **Type**.

5. Double-cliquez sur **Insérer une nouvelle ligne**.

6. Sélectionnez une politique d'authentification dans la liste et sélectionnez .

Remarque :
Ne sélectionnez pas **Politique d'accès** autorisée ou **Politique d'accès refusée**. Ces politiques ne sont destinées qu'aux connexions des utilisateurs.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

Lorsqu'il y a un changement dans le profil d'authentification, l'en-tête d'autorisation renvoie une valeur spécifique aux changements apportés à ce moment-là. Pour pouvoir obtenir tous les schémas d'authentification renvoyés dans l'en-tête « WWW-Authenticate », vous devez activer `glide.security.response.authenticate.header.auth_profile.first_scheme_only` sur **faux**. La réponse est renvoyée avec plusieurs en-têtes. Par exemple :

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une politique d'accès de l'API SOAP

Créez une politique d'accès API et mappez un profil d'authentification pour restreindre le type d'authentification d'une API SOAP. Par exemple, vous pouvez créer une politique d'accès d'API qui autorise uniquement l'authentification par jeton d'ID pour une API SOAP.

Avant de commencer

- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, voir Créer un profil d'authentification.
- Rôle requis : admin

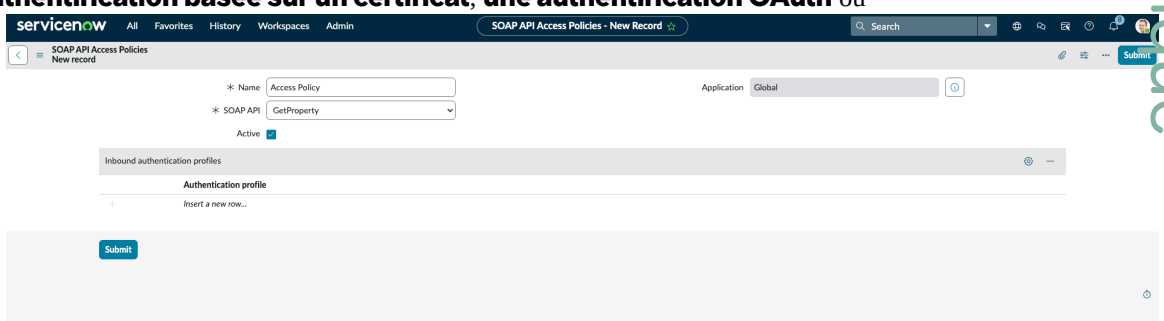
Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Politiques d'accès de l'API SOAP**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès API.
API SOAP	API SOAP à laquelle la politique d'accès est appliquée. Par exemple, **l'API GetProperty**.
Application	Périmètre de l'application.
Actif	Option pour rendre la politique d'accès API active.

4. Dans la section Authentification entrante, double-cliquez sur **Insérer une nouvelle ligne**.
5. Sélectionnez un profil d'authentification entrant dans la liste et cliquez sur l'icône .
   Par exemple, vous pouvez ajouter **une authentification de base**, **un jeton d'ID**, **une authentification basée sur un certificat**, **une authentification OAuth** ou **WSSE**.



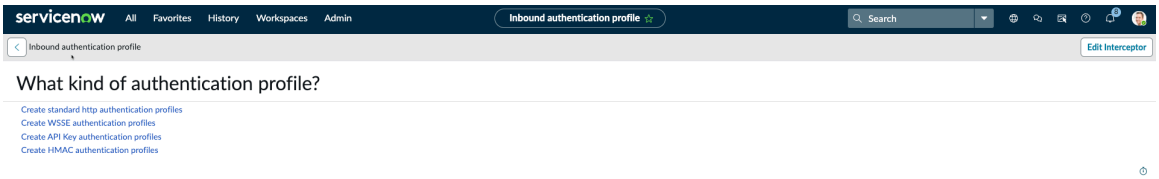
   a. Pour ajouter un ou plusieurs profils d'authentification entrants, cliquez sur **Nouveau** pour créer un profil.

   b. **Choisir quel type de profils d'authentification ?**

   - **Créer des profils d'authentification http standard**
   - **Créer des profils d'authentification WSSE**

Traduction automatique

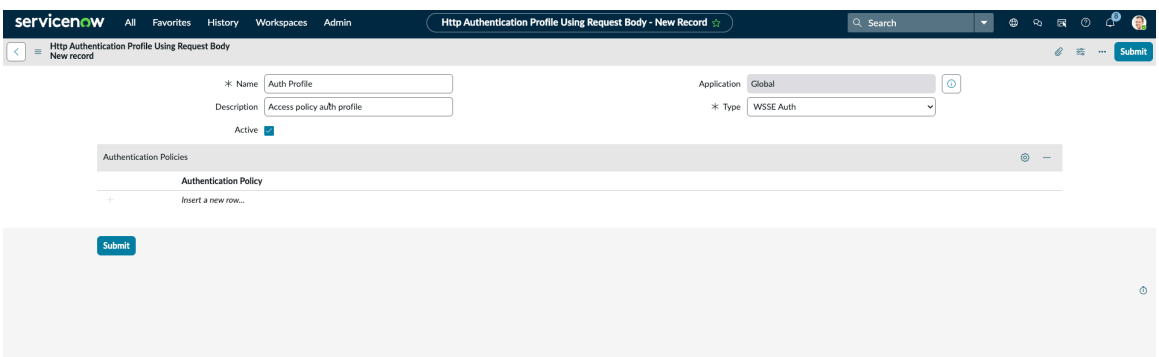
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Pour créer un profil d'authentification WSSE, renseignez les champs du formulaire.

Profil d'authentification WSSE

Champ	Description
Nom	Nom unique de la politique d'accès API.
Description	Description du profil d'authentification.
Application	Périmètre de l'application.
Actif	Option pour rendre la politique d'accès API active.
Type	Authentification WSSE en tant que profil d'authentification WSSE (sécurité Web).



d. Après avoir créé le profil d'authentification, enregistrez l'enregistrement.

6. Cliquez sur **Soumettre** pour soumettre la politique d'accès de l'API SOAP.

Créer une politique globale d'accès aux API pour protéger les API SOAP

Créez une politique d'accès API globale unique pour protéger toutes les API SOAP.

Avant de commencer

- Rôle requis : admin
- Installer le module d'extension **Processor Access policy** (com.glide.processor.policy)
- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, voir Créer un profil d'authentification.

Les étapes suivantes décrivent comment créer une politique d'accès globale unique pour protéger toutes les API SOAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

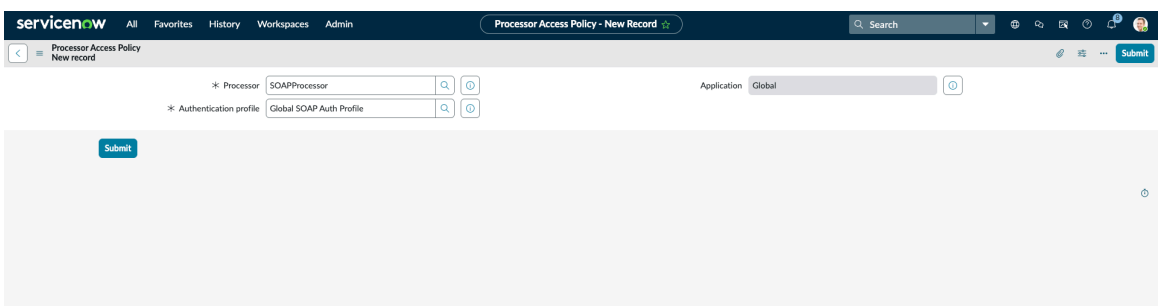
Remarque :
Les politiques définies aux niveaux individuels de l'API SOAP remplacent la politique d'accès globale de niveau **SOAPProcessor** .

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Politiques d'accès aux processus**.
2. Remplissez les champs du formulaire.

Formulaire de politique d'accès au processus

Champ	Description
Processeur	Nom permettant d'identifier la politique d'authentification. Par exemple, sélectionnez **SOAPProcessor** (profil d'authentification).
Application	Périmètre de la politique d'authentification. Par défaut : global
Profil d'authentification	Type du profil d'authentification. Sélectionnez, **Profil d'authentification SOAP global**.



3. Sélectionnez **Soumettre**.

Critères de filtre pour les API

Les critères de filtre contiennent des conditions de filtre ou des requêtes qui sont utilisées comme entrées de politique pour une politique d'authentification. Les entrées de politique sont utilisées pour regrouper un ou plusieurs critères de filtre et définir les conditions de politique d'une politique d'authentification. Par exemple, un critère de filtre d'adresses IP définit une adresse IP au format CIDR (Classless Inter-Domain Routing) ou une plage d'adresses IP.

Vous pouvez créer des critères de filtre basés sur l'adresse IP de l'utilisateur, son rôle et le groupe d'utilisateurs auquel il appartient.

Remarque :
Vous utilisez également les critères de filtre créés à partir du module **Authentification adaptative** . Pour plus d'informations, consultez Authentification adaptative.

Vous pouvez créer des critères de filtre pour les API à l'aide du même processus que les critères de filtre pour l'authentification adaptative. Pour obtenir des détails, consultez Critère de filtre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Créer un critère de filtre d’adresses IP

Créer un critère de filtre de rôle

Créer des critères de filtre de groupe

Politiques d'authentification API

Les politiques d’authentification évaluent les demandes d’authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l’accès en fonction des critères de correspondance.

Vous pouvez utiliser la politique de blocage globale intégrée ou créer une politique d’authentification en fonction de vos besoins de sécurité. La politique de blocage globale refuse les demandes d’authentification des utilisateurs et des API en fonction des critères de filtre spécifiés.

Remarque :
N’utilisez pas et ne modifiez pas la politique d’autorisation d’accès et la politique de refus d’accès. Ces politiques ne sont destinées qu’aux connexions des utilisateurs.

Créer une politique d’authentification API

Les politiques d’authentification vous permettent d’appliquer des restrictions d’accès sur les API en fonction des critères de filtre spécifiés.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politique d'authentification API**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire de police

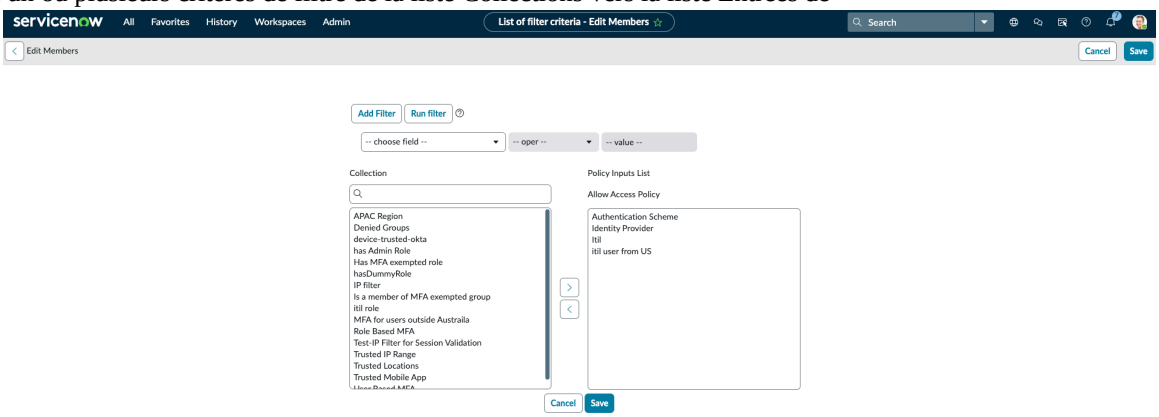
Champ	Description
Nom	Nom permettant d’identifier la politique.
Description	Brève description de la politique.
Application	Périmètre de l'application.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. Dans l’onglet Entrées de politique, sélectionnez **Modifier** pour ajouter les critères de filtre existants.
   Vous pouvez également créer une nouvelle entrée de politique. Pour plus d’informations, consultez Créer des entrées de politique .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Déplacez un ou plusieurs critères de filtre de la liste Collections vers la liste Entrées de

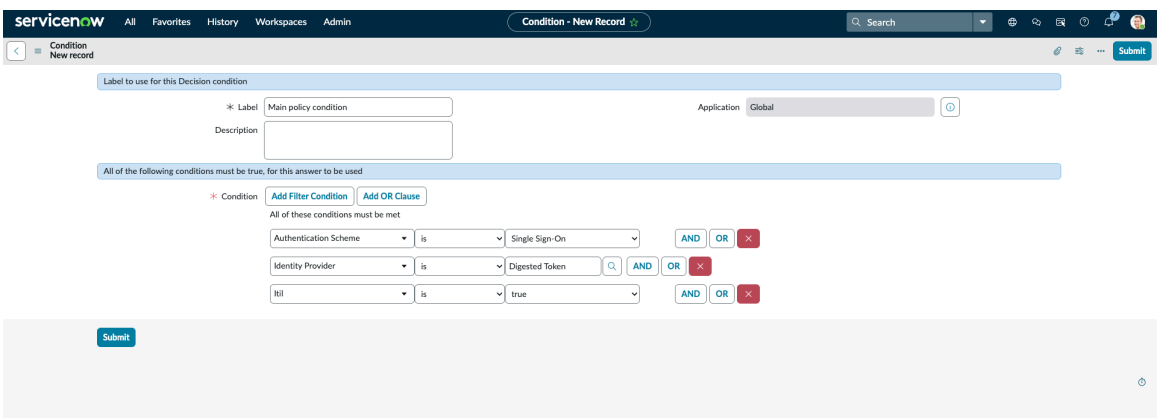


politique.

7. Sélectionnez **Enregistrer**.
8. Dans l'onglet Conditions de la politique, sélectionnez **Nouveau**.
9. Renseignez ces champs du formulaire.

Formulaire Condition

Champ	Description
Étiquette	Nom de la condition de la politique.
Description	Brève description de la condition de la politique.
Application	Périmètre de l'application.
Condition	Une ou plusieurs conditions combinées avec le filtre **OU** .



10. Sélectionnez **Soumettre**.

Configurer la politique de blocage globale pour les API

La politique de blocage globale refuse les demandes d'authentification des utilisateurs et des API en fonction des conditions de politique spécifiées. Cette politique peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Politique de blocage globale**.
2. Dans l'onglet **Entrées de politique** , cliquez sur **Modifier**.
3. Sélectionnez un ou plusieurs critères de filtre dans la liste **Collection** et déplacez-les vers la liste **Politique de blocage globale** .
   Vous pouvez également ajouter des filtres supplémentaires.
4. Dans l'onglet **Conditions de la politique** , cliquez sur **Nouveau**.
5. Renseignez les champs suivants du formulaire :

Formulaire de condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtre) utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires à partir d'une liste d'adresses IP de confiance.

Politique d'accès pour le système ou les processeurs d'exportation

Possibilité pour les processeurs système ou d'exportation de tirer parti de la politique d'accès du processeur pour sécuriser tous les points de terminaison d'exportation.

Capacité à sécuriser tous les points de terminaison d'exportation et à appliquer le profil d'authentification entrant et les politiques d'accès au processeur au niveau global ou d'instance.

Remarque :

- Les processeurs non publics, y compris les processeurs d'exportation tels que CSV, PDF, et autres, sont pris en charge pour les stratégies d'accès.
- Les scripts processeurs sont également pris en charge pour les stratégies d'accès.

Exemples de cas d'utilisation

- L'administrateur peut bloquer le processeur RSS s'il n'a pas l'intention de l'utiliser, en tirant parti de la politique d'accès API.
- L'administrateur peut créer un profil d'authentification avec une authentification de base et associer une politique d'authentification qui est toujours évaluée sur faux.

  Par exemple, créez des critères d'adresse IP avec une plage comprise entre `0.0.0.0` et `255.255.255.255` (ajoutez également l'espace d'adressage Ipv6), puis ajoutez une condition de politique avec l'opérateur faux. De cette façon, les conditions de la politique seront toujours évaluées comme fausses et la politique d'accès de l'API bloquera l'accès, quelle que soit l'origine de la demande.

- Autoriser l'accès au processeur uniquement à partir d'un réseau de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer la politique d'accès au processeur

Pour Processeur, installez le module d'extension Politique d'accès au processeur (com.glide.processor.policy).

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Les éléments suivants sont installés avec la politique d'accès au processeur :

- Propriété système : com.glide.auth.profile.supported.processor.list
- Module dans la navigation : Politiques d'accès au processeur

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Processor Access Policy (com.glide.processor.policy) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Que faire ensuite

.
Configurez le profil d'authentification pour les processeurs. Pour plus d'informations, Configurer le profil d'authentification du processeur reportez-vous à la section .

Configurer le profil d'authentification du processeur

Appliquez le profil d'authentification pour les processeurs d'exportation.

Avant de commencer
Rôle requis : admin

Module d'extension requis : Politique d'accès au processeur (com.glide.processor.policy)

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Politiques d'accès au processeur**.
2. Pour ajouter un profil d'authentification au processeur, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Traduction automatique

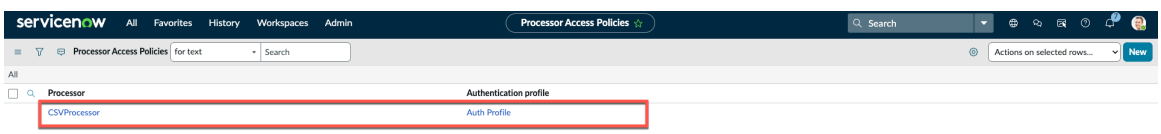
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de politique d'accès au processus

Champ	Description
Processeur	Nom permettant d'identifier la politique d'authentification. **Remarque :** Les processeurs publics ne sont pas pris en charge. Si un processeur non pris en charge est sélectionné, une erreur s'affiche lors de la soumission du processeur.
Application	Périmètre de la politique d'authentification. Par défaut : global
Profil d'authentification	Type du profil d'authentification. Vous pouvez sélectionner **Jeton d'ID** ou **Jeton OAuth**.

4. Cliquez sur **Envoyer**.
   Le profil d'authentification est appliqué au processeur.

   Par exemple, le profil d'authentification OAuth est configuré pour le processeur CSV. Dans ce cas, vous devez utiliser le jeton d'accès OAuth pour l'exportation en utilisant CSV comme option d'exportation.



Authentification basée sur certificat

L'authentification basée sur certificat vous permet d'authentifier mutuellement les connexions des utilisateurs ou les demandes d'API entrantes à l'aide de certificats d'une autorité de certification (CA) approuvée.

Remarque :
L'authentification basée sur certificat n'est pas prise en charge sur les instances sur site et Edge Encryption.

Authentification basée sur certificat pour les connexions à l'interface utilisateur

Permettez aux utilisateurs finaux d'utiliser des cartes PIV (vérification de l'identité personnelle) ou CAC (Common Access Card) pour se connecter au ou Portail de services au lieu d'utiliser un nom d'utilisateur et un ServiceNow AI Platform mot de passe. Pour configurer l'authentification réciproque pour les connexions d'interface utilisateur, reportez-vous à la section Configurer l'authentification basée sur certificat.

Une fois l'authentification basée sur certificat configurée, les utilisateurs finaux peuvent finaliser leur configuration et se connecter. Consultez Se connecter à l'aide de l'authentification basée sur certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification basée sur certificat pour les services Web entrants

Authentifiez les demandes entrantes vers ServiceNow les API SOAP et REST. Pour configurer l'authentification réciproque des services Web entrants, reportez-vous à la section Configurer l'authentification basée sur certificat.

Configurer l'authentification basée sur certificat

Configurez l'authentification réciproque pour les connexions basées sur l'interface utilisateur ou les services Web entrants.

Avant de commencer

Rôle requis : admin

Vérifiez que votre instance utilise un équilibreur de charge ADCv2. Pour plus d'informations, consultez l'article de labase de connaissances sur la migration ADCv2. Si votre instance n'utilise pas l'équilibreur de charge ADCv2, contactez Now Support.

Procédure

Configurez l'authentification basée sur certificat pour :

- Autorisez les utilisateurs finaux à se connecter en toute sécurité à ou à l'aide des ServiceNow AI PlatformPortail de services cartes PIV ou CAC. Une fois l'authentification basée sur certificat activée, vous pouvez enregistrer automatiquement le certificat PEM ou un administrateur peut mapper le certificat pour vous. Consultez Se connecter à l'aide de l'authentification basée sur certificat.
- Activez l'authentification réciproque pour les services Web entrants. Une fois l'authentification basée sur certificat configurée, le système utilise les certificats fournis pour authentifier mutuellement les demandes d'accès ServiceNow aux API REST et SOAP.

Activer l'authentification basée sur certificat

Vous pouvez activer le module d'extension Authentification basée sur certificat (com.glide.auth.mutual) si ServiceNow AI Platform vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Les tables suivantes sont installées avec l'authentification basée sur certificat :

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension d'authentification basée sur certificat (com.glide.auth.mutual) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Enregistrer le certificat de l'autorité de certification

Enregistrez les certificats racines ou intermédiaires pour qu'ils soient disponibles à l'authentification.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification basée sur certificat** > **Chaîne de certificats CA**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire Certificat d'authentification de l'autorité de certification mutuelle

Champ	Description
Nom	Nom permettant d'identifier le certificat.
Notification d'échéance	Option permettant d'avertir les utilisateurs lorsqu'un certificat est sur le point d'expirer.
Notification à l'expiration	Liste des utilisateurs à notifier lorsque le certificat expire.
Avertissement avant l'expiration (en jours)	Nombre de jours pendant lesquels une notification est envoyée aux utilisateurs avant l'expiration d'un certificat.
Actif	Option permettant d'activer le certificat client.
Format	PEM
Type	Type de certificat. Les options incluent : ○ **Certificat de l'autorité** de certification : certificat de l'autorité de certification racine. Peut également inclure des certificats intermédiaires dans la chaîne. Les certificats CA sont automatiquement synchronisés avec l'équilibreur de charge. Utilisez cette option dans la mesure du possible pour éviter de manquer un certificat requis dans la chaîne. ○ **Certificat intermédiaire** : certificat intermédiaire dans la chaîne de certifications. Ce certificat reste sur l'instance uniquement et n'est pas synchronisé avec l'équilibreur de charge. N'utilisez cette option que si vous devez ajouter un certificat intermédiaire à une chaîne existante.
Description brève	Brève description du certificat client de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pendant le chargement du certificat, les champs en lecture seule **Valide à partir de**, **Expire,Expire dans les jours**, **Émetteur** et **Objet**, **Chaîne du certificat** et **Certificat PEM** sont extraits et renseignés automatiquement.

4. Cliquez sur **Envoyer**.
5. **Facultatif :** Cliquez sur **Valider les banques/certificats** pour valider le certificat.

Mapper le certificat PEM à l'utilisateur

Mappez les certificats PEM aux utilisateurs pour leur permettre de se connecter à l'aide de cartes PIV ou CAC ou d'authentifier les demandes entrantes. Vous pouvez mapper plusieurs certificats PEM à un utilisateur.

Avant de commencer

- Rôle requis : admin
- Assurez-vous d'avoir le certificat PEM (Privacy Enhanced Mail) de l'utilisateur.

Remarque :
Après avoir mappé le certificat PEM à la configuration utilisateur, la « vérification du certificat » échoue. Cela est dû au fait que le certificat PEM n'est pas stocké.

Procédure

1. Accédez à la **Tous** > **Authentification basée sur certificat** > **Utilisateur vers Mappage de certificat** et cliquez sur **Nouveau**.
2. Renseignez les champs suivants du formulaire :

Formulaire Certificat client de l'utilisateur

Champ	Description
Nom	Nom du certificat client de l'utilisateur.
Notification d'échéance	Option permettant d'avertir les utilisateurs lorsqu'un certificat est sur le point d'expirer.
Avertissement avant l'expiration (en jours)	Nombre de jours pendant lesquels une notification est envoyée aux utilisateurs avant l'expiration d'un certificat.
Notification à l'expiration	Liste des utilisateurs à notifier lorsque le certificat expire.
Actif	Option permettant d'activer le certificat client.
Utilisateur	Utilisateur mappé au certificat client. Le système reçoit le certificat client à partir de la demande entrante ou de l'enregistrement du certificat, puis utilise l'utilisateur désigné dans ce champ pour lancer une session afin d'exécuter la demande.
Description brève	Brève description du certificat client de l'utilisateur.
Format	Le format PEM (Privacy Enhanced Mail) est un certificat DER (Distinguished Encoding Rules) codé en base 64.
Type	Cert. client Ce champ est en lecture seule.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pendant le chargement du certificat, les champs en lecture seule **Valide à partir de**, **Expire,Expire dans les jours**, **Émetteur** et **Objet** sont extraits et renseignés automatiquement.

3. Cliquez sur l'icône Pièces jointes et chargez le certificat.
4. Cliquez sur **Envoyer**.
   Le certificat est validé et mappé à l'utilisateur spécifié si le certificat provient d'une autorité de certification (CA) approuvée.

Configurer les propriétés d'authentification basée sur certificat

Utilisez les propriétés système pour activer ou désactiver les fonctionnalités d'authentification basées sur certificat.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification basée sur certificat** > **Propriétés**.
2. Renseignez les champs suivants du formulaire :

Formulaire Propriétés de l'authentification basée sur certificat

Propriété	Description
Activer l'authentification basée sur certificat	Option permettant d'activer l'authentification basée sur certificat pour les connexions à l'interface utilisateur et les services Web entrants. Par défaut : true
Afficher l'option « Se connecter avec PIV/CAC » sur l'écran de connexion	Affiche l'option **Se connecter avec la carte PIV/CAC** sur l'écran de connexion. Permet aux utilisateurs de se connecter à l'aide de l'authentification basée sur certificat à l'aide de l'interface utilisateur. Valeur par défaut : false
Activer la redirection automatique pour la connexion basée sur certificat	Détermine s'il faut exiger que l'utilisateur clique sur **Se connecter avec la carte PIV/CAC** après avoir sélectionné un certificat enregistré et saisi son code PIN. Activez cette option pour connecter automatiquement l'utilisateur une fois qu'il a sélectionné un certificat client enregistré et saisi son code PIN. Désactivez pour exiger que l'utilisateur clique sur **Se connecter avec la carte PIV/CAC** après avoir sélectionné un certificat client enregistré et saisi son code PIN. Valeur par défaut : false

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se connecter à l'aide de l'authentification basée sur certificat

Une fois que votre administrateur a configuré l'authentification basée sur certificat, vous pouvez enregistrer le certificat client et vous connecter à l'aide de votre carte PIV (Personal Identity Verification) ou CAC (Common Access Card).

Enregistrer un certificat client pour votre carte PIV ou CAC

Avant de vous connecter à l'aide de ServiceNow AI Platform votre carte PIV ou CAC, vous devez enregistrer le certificat client de votre carte PIV ou CAC. Si vous ne parvenez pas à enregistrer le certificat client, contactez votre administrateur. Votre administrateur peut également enregistrer le certificat client de votre carte PIV ou CAC.

Avant de commencer

- Assurez-vous que l'authentification basée sur certificat est activée.
- Assurez-vous qu'un lecteur de carte est connecté à votre ordinateur et que votre carte PIV ou CAC est insérée.
- Rôle requis : aucun

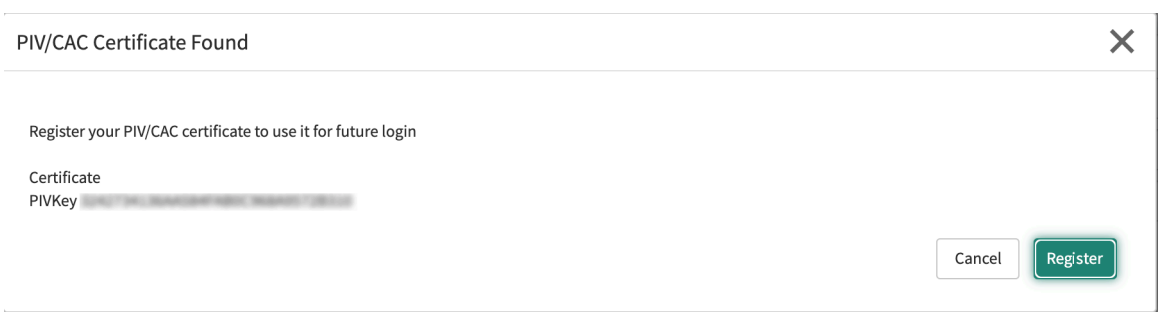
Pourquoi et quand exécuter cette tâche

Si vous avez besoin d'un administrateur pour enregistrer votre certificat client, reportez-vous à la section Mapper le certificat PEM à l'utilisateur.

Procédure

1. Connectez-vous à l'aide de votre nom d'utilisateur et de ServiceNow AI Platform votre mot de passe.
2. Cliquez sur votre nom dans le **menu utilisateur** et sélectionnez **Profil**.
3. Dans les **liens connexes**, cliquez sur **Enregistrer le certificat client**.

   Si un certificat valide est disponible, le message suivant s'affiche :



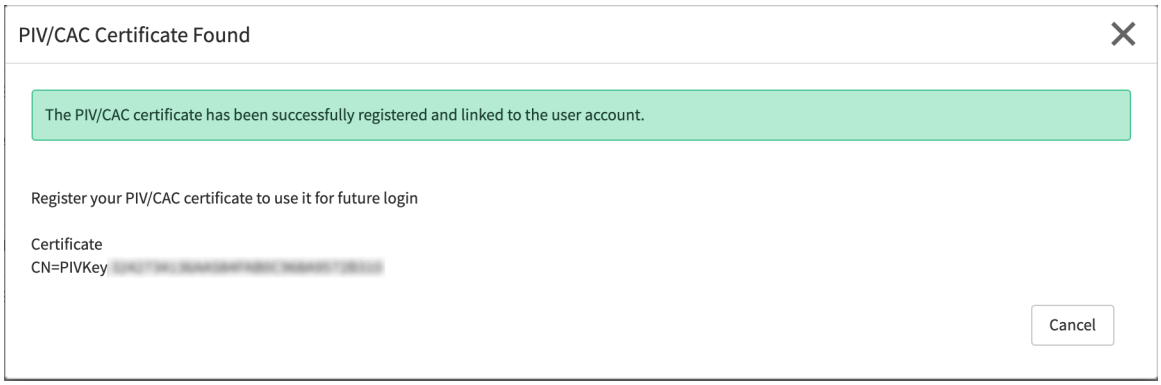
4. Cliquez sur **Inscrire**.

   Une fois l'inscription réussie, le message suivant s'affiche :

   Le certificat PIV/CAC a été correctement enregistré et lié au compte utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La prochaine fois que vous vous connecterez à votre ServiceNow AI Platform, vous pourrez vous connecter à l'aide de votre carte PIV ou CAC. Pour plus d'informations, consultez Connectez-vous à l'aide de la ServiceNow AI Platform carte PIV ou CAC.

Connectez-vous à l'aide de la ServiceNow AI Platform carte PIV ou CAC

Vous pouvez vous connecter avec votre carte PIV ou CAC au lieu du nom d'utilisateur et du mot de passe lorsque l'authentification basée sur certificat est activée sur ServiceNow AI Platform.

Avant de commencer

- Rôle requis : aucun
- Assurez-vous que l'authentification basée sur certificat est activée.
- Assurez-vous qu'un lecteur de carte PIV ou CAC est connecté à votre ordinateur.
- Assurez-vous qu'un certificat client de votre carte PIV ou CAC vous est mappé. Pour plus d'informations, consultez Enregistrer le certificat de l'autorité de certification.

Procédure

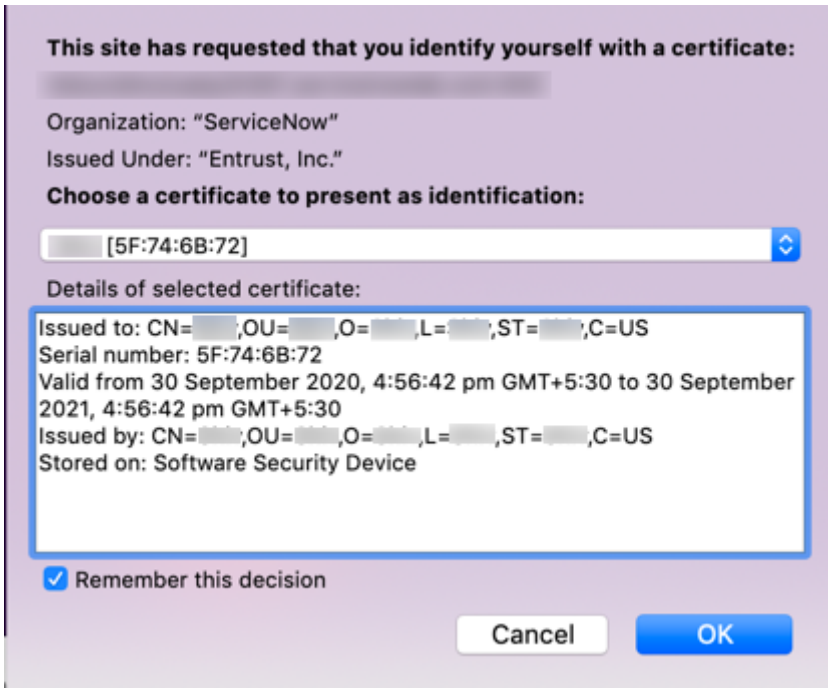
1. Insérez votre carte PIV ou CAC dans le lecteur de carte.
2. Accédez à votre instance dans un navigateur.
   Le navigateur vous invite à entrer un code PIN pour votre carte PIV ou CAC.
3. Entrez le code PIN de votre carte PIV ou CAC dans l'invite du navigateur.

   Remarque :
   Si vous oubliez votre code PIN, contactez votre administrateur.

4. Si vous saisissez un code PIN correct, le navigateur affiche une invite pour sélectionner un certificat.

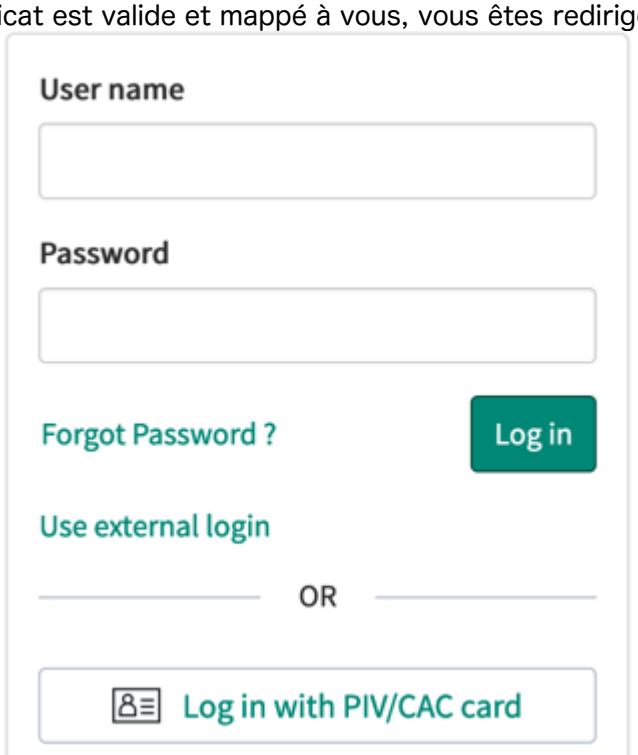
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez un certificat dans l'invite du navigateur.

   Si le certificat est valide et mappé à vous, vous êtes redirigé vers la page de connexion.



6. Cliquez sur **le bouton Se connecter avec la carte PIV/CAC** .

   Pour vous déconnecter du , vous devez supprimer le PIV ou le CAC du lecteur de ServiceNow AI Platform carte, puis fermer le navigateur.

Gérer vos certificats clients

Affichez et supprimez les certificats clients associés à votre compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Assurez-vous que l'authentification basée sur certificat est activée.
- Rôle requis : aucun

Procédure

1. Connectez-vous à l'aide de votre nom d'utilisateur et de ServiceNow AI Platform votre mot de passe.
2. Cliquez sur votre nom dans le **menu utilisateur** et sélectionnez **Profil**.



3. Dans les **liens connexes**, cliquez sur **Gérer vos certificats clients**.
   La table Certificats clients utilisateurs [sys_user_certificate] s'ouvre et affiche les certificats associés à votre compte.
4. Affichez ou supprimez les certificats associés à votre compte.

URL d'instances personnalisées

Vous pouvez activer l'accessibilité de votre ServiceNow instance à partir d'une URL personnalisée ou de marque de l'entreprise.

Vue d'ensemble des URL personnalisées

Vous pouvez utiliser une URL personnalisée pour permettre ServiceNow à l'instance d'être accessible à partir d'une ou de plusieurs URL de marque d'entreprise ou personnalisées.

Les URL personnalisées peuvent être associées à un portail spécifique. Par exemple, l'administrateur peut définir http://support.acme.com pour le portail CSM et http://hr.acme.com pour le portail RH. Dans ce cas, il est nécessaire de rediriger les utilisateurs vers différents fournisseurs d'identités pour l'authentification en fonction de l'URL personnalisée à laquelle ils accèdent.

Important :

- Ne créez pas d'URL personnalisée avec plus de 100 domaines par instance.
- Vous devez d'abord supprimer l'enregistrement d'URL personnalisée de l'instance ServiceNow , puis supprimer toutes les entrées DNS (Domain Name Server) du serveur DNS.
- Toute suppression de l'entrée DNS du serveur DNS avant la suppression de l'enregistrement d'URL personnalisée de ServiceNow l'instance entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisée correspondants de ServiceNow.

À partir de Tokyo, vous pouvez autoriser les utilisateurs à rediriger automatiquement vers les fournisseurs d'identités spécifiés définis dans l'enregistrement d'URL personnalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les URL personnalisées ne sont pas disponibles pour les clients sur site ou les instances de développeur. De plus, l'URL doit être accessible au public.

Seul le propriétaire du domaine de niveau supérieur (TLD) ou de tout sous-domaine peut configurer l'URL personnalisée en sous-domaine DNS. Par exemple, votre instance peut avoir l'URL désignée suivante et d'autres URL personnalisées :

Exemple d'URL personnalisée

Exemples d'URL	Utilisation
https://acme.service-now.com	Nom de domaine initial pour ACME fourni avec l'instance ServiceNow .
https://support.acme.com	URL personnalisée qui s'associe à votre ServiceNow instance. Cette URL est appelée alias (CNAME) du nom de domaine initial.
https://US-support.acme.com	URL personnalisée secondaire qui s'associe à un portail de services sur votre instance. Votre instance peut prendre en charge plusieurs URL personnalisées vers le même portail de services.

Considérations relatives aux URL personnalisées en dehors de votre instance

Avant de pouvoir associer une URL personnalisée, vous devez posséder (ou acheter) une URL par l'intermédiaire d'un fournisseur de domaine. Il existe également des configurations spécifiques nécessaires avant de pouvoir créer et associer une URL personnalisée sur votre instance.

Configurations d'URL personnalisées

Éléments de configuration	Description
Définir le CNAME avec le fournisseur	L'enregistrement CNAME doit être défini comme URL d'instance ServiceNow .
Déterminez votre statut VIP dédié	Le statut de VIP.

Remarque :
Lors de la suppression ou de la mise à jour des enregistrements CNAME qui pointent vers votre instance, vous devez suivre cette séquence pour éviter les enregistrements non résolus dans l'instance. Tout d'abord, supprimez les enregistrements CNAME de votre instance, puis supprimez ou mettez à jour le paramètre CNAME de votre fournisseur DNS.

Activer les URL personnalisées

Activez la configuration d'URL personnalisées sur votre ServiceNow instance. Vous pouvez activer le module d'extension URL personnalisée (com.snc.customurl) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**.
2. Recherchez et cliquez sur le module d'extension **URL personnalisée** .

> **Remarque :**
> Ne sélectionnez pas le module **d'extension URL personnalisée - Interne** , qui est un composant interne pour les API d'URL personnalisées scriptées.

3. Dans l'enregistrement URL personnalisée, cliquez sur le lien connexe **Activer/Réparer** .
4. Dans la fenêtre Activation du module d'extension, cliquez sur **Activer**.
   Lorsque la fenêtre d'activation du module d'extension s'ouvre à nouveau avec un message indiquant que le module d'extension est activé, cliquez sur **Fermer et recharger le formulaire** pour rester sur ce formulaire.
5. Dans la liste connexe Fichiers de module d'extension, recherchez la propriété suivante et modifiez la valeur du paramètre :

Option	Description
glide.customurl.enabled	Pour activer les URL personnalisées, définissez la valeur sur **Vrai**. Par défaut, cette propriété est définie sur **Faux**, ce qui signifie que vous ne pouvez pas associer d'URL personnalisée. **Remarque :** Pour désactiver cette fonctionnalité, redéfinissez cette propriété sur **Faux**.

6. Cliquez sur **Mettre à jour**.

Définir une URL personnalisée comme URL d'instance

Ajoutez une URL personnalisée à votre configuration d'instance à utiliser à la place de votre ServiceNow URL.

Avant de commencer

Rôle requis : admin

Vous devez activer le module d'extension URL personnalisée et avoir acheté ou enregistré une URL avant d'ajouter l'URL personnalisée à votre instance.

Procédure

1. Accédez à la **Tous** > **URL personnalisée** > **URL personnalisées**.
2. Vous devez soit :
   - Cliquez sur **Nouveau** pour associer un nouveau nom de domaine nouveau dans votre instance.
   - Sélectionnez une URL personnalisée déjà configurée à définir en tant qu'URL d'instance.
3. Renseignez les champs appropriés :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'URL personnalisés

Champ	Description
Nom du domaine	Nom de domaine complet (FQDN) de l'URL personnalisée. Le FQDN est une redirection CNAME créée dans l'enregistrement du serveur de noms pour le domaine personnalisé. **Remarque :** Par exemple, dans le serveur de noms de acme.com, vous pouvez créer une entrée : `support.acme.com 300 IN CNAME acme.servicenow.com`
Est une URL d'instance	Cochez la case pour activer cette URL personnalisée pour toutes les URL sortantes. Une seule URL personnalisée active peut être l'URL d'instance. Pour activer ce paramètre pour une URL personnalisée, cliquez sur **Définir en tant qu'URL d'instance** dans l'enregistrement d'URL. Toutes les URL personnalisées précédentes sont alors supprimées.
Statut	État de l'enregistrement d'URL personnalisée. Si l'état est **Actif**, l'URL personnalisée est mise en service et prête à l'emploi.
Portail de services	Portail de services que vous souhaitez utiliser lorsque vous redirigez les utilisateurs vers votre instance à l'aide de l'URL personnalisée.
Fournisseur d'identité	Le fournisseur d'identité de l'URL personnalisée vous permet d'autoriser les utilisateurs à être redirigés automatiquement vers les fournisseurs d'identité spécifiés définis dans l'enregistrement de l'URL personnalisée.

Une URL personnalisée doit être activée dans les six heures sur votre instance.

Remarque :

- Vous devez d'abord supprimer l'enregistrement d'URL personnalisée de l'instance ServiceNow , puis supprimer toutes les entrées DNS (Domain Name Server) du serveur DNS.
- Toute suppression de l'entrée DNS du serveur DNS avant la suppression de l'enregistrement d'URL personnalisée de ServiceNow l'instance entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisée correspondants de ServiceNow.

URL personnalisée avec fournisseur d'identité

Définissez votre URL personnalisée avec le fournisseur d'identité pour permettre à l'utilisateur de se connecter avec son fournisseur d'identité.

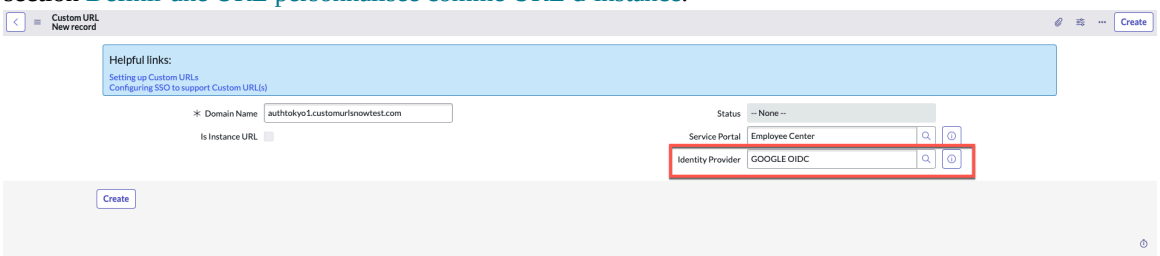
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

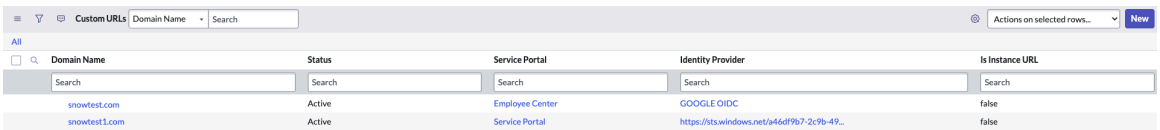
Procédure

1. Accédez à la **Tous** > **URL personnalisée** > **URL personnalisées**.
2. Cliquez sur **Nouveau**.
3. Fournissez les détails de l'IdP dans le champ **Fournisseur d'identité** .
   Pour plus d'informations sur les autres champs, reportez-vous à la section Définir une URL personnalisée comme URL d'instance.



4. Cliquez sur **Créer**.

   L'enregistrement est créé et affiché sur la page URL personnalisée.



   Lorsque l'URL personnalisée est accessible, l'utilisateur est redirigé vers le fournisseur d'identité configuré. Dans ce cas, en accédant au snowtest.com, l'utilisateur est dirigé vers le **Centre des employés**, puis redirigé vers le fournisseur d'identité Google .

   Remarque :

   - Si le Portail de services champ est vide et que le champ Fournisseur d'identité est défini, lorsque l'utilisateur accède à l'URL personnalisée, il est directement dirigé vers le fournisseur d'identité configuré.
   - Si le champ Fournisseur d'identité Portail de services est défini, lorsque l'utilisateur accède à l'URL personnalisée avec le Portail de services qui est défini, il est dirigé vers le fournisseur d'identité configuré.
   - Si le champ Fournisseur d'identité Portail de services est défini, lorsque l'utilisateur accède à l'URL personnalisée avec un portail différent qui n'est pas défini, il est dirigé vers le fournisseur d'identité de redirection automatique s'il est configuré sur l'instance.

5. Utilisez les informations d'identification pour vous connecter à l'application.

URL personnalisée Informations sur la tâche de centre de données

Chaque URL personnalisée associée à votre instance a une tâche de centre de données ServiceNow correspondante qui s'exécute et affiche les informations d'URL pertinentes pour votre instance, comme décrit dans la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ de tâche	Description
ID de tâche	ID unique de la tâche qui vérifie le domaine de l'URL personnalisée.
Dernière exécution à	Date et heure de la dernière exécution de la tâche.
Charge utile	Liste de domaines ou d'URL personnalisées qui ont été envoyés au centre de données pour la mise en service de CERT.
Nombre d'interrogations	Nombre de fois où les résultats ont fait l'objet d'une interrogation pour cette tâche.
Résultat	Vérifie et valide chaque domaine ou URL personnalisée envoyé dans une charge utile.
Statut	Statut de la tâche du centre de données.

Générer les métadonnées SP pour les installations d'URL personnalisées SAML/SSO

Une installation SAML ou SSO nécessite que les métadonnées SP soient générées pour l'IdP avant la génération de l'instance d'URL personnalisée.

Avant de commencer

Rôle requis : admin

L'IdP a besoin des métadonnées SP pour l'instance afin d'authentifier et de transmettre les demandes.

Remarque :
L'ajout de l'URL de service consommateur d'assertion (URL de connexion du SP) peut être différent pour chaque fournisseur d'identités (Azure, ADFS ou Okta).

Procédure

1. Choisissez votre module d'extension SSO installé :

Option	Description
Authentification unique (SSO) de plusieurs fournisseurs	Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**. Choisissez un IdP et cliquez sur le bouton **Générer les métadonnées** . L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres de propriété système.
SAML 2 SSO	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres de propriété système.

2. Copiez les métadonnées SP dans la zone de texte.

Par exemple :

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://yourinstance.service-now.com">
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
 <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
 <AssertionConsumerService isDefault="true" index="0"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/navpage.do" />
 <AssertionConsumerService index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Fournissez les métadonnées du SP d'instance à l'IdP.
   Par exemple, SSOCircle permet à un utilisateur de fournir les métadonnées SP en ligne.
4. **Facultatif :** Pour configurer des URL personnalisées dans Azure :
   a. Accédez à **Inscriptions d'applications**.
   b. Sélectionnez **Toutes les applications** dans le menu.
   c. Sélectionnez **l'application ServiceNow**.
   d. Cliquez sur Paramètres pour configurer l'URL.
5. **Facultatif :** Pour configurer des URL personnalisées dans Okta :
   a. Créez deux ServiceNow applications UD Okta.
   b. Une application Okta pour l'URL d'instance « service-now.com ».
   c. Une application Okta pour l'URL personnalisée.

   Remarque :
   - Désactivez **l'option Désactiver l'authentification forcée** dans la configuration Okta pour que le Test de la **connexion** s'exécute correctement.
   - Si vous testez l'enregistrement de fournisseur d'identité associé à l'URL de base, assurez-vous de disposer d'une connexion à l'instance avec l'URL de base.
   - Si vous testez le fournisseur d'identité associé à l'URL personnalisée, assurez-vous de disposer d'une connexion à l'instance avec l'URL personnalisée.
6. **Facultatif :** Pour utiliser l'authentification OAuth, configurez l'URL de redirection comme toutes les URL personnalisées enregistrées dans la configuration du point de terminaison de l'application OAuth pour les applications clientes externes.
   L'URL de redirection est synonyme de l'URL de rappel vers laquelle le serveur d'autorisation redirige.
7. **Facultatif :** Pour utiliser le service Google reCAPTCHA, configurez une paire de clés API.

Erreurs et correctifs d'URL personnalisée

Une liste des erreurs courantes et des correctifs associés pour une installation et une configuration d'URL personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration

Message d'erreur	Corriger
Impossible de créer une URL personnalisée. Réessayez ultérieurement.	Il peut y avoir un problème indépendant de votre volonté qui interfère avec la création de l'URL personnalisée. Exécutez à un autre moment avant de contacter le support. **Remarque :** La création d'une URL personnalisée prend généralement 30 minutes. Si cela prend plus de temps, contactez https://support.servicenow.com/now?draw=case.
Impossible de soumettre votre nouvelle demande URL personnalisée, car une autre demande URL personnalisé pour votre instance est toujours en cours.	Vérifiez l'état de vos tâches d'URL personnalisée avant de soumettre une nouvelle demande.
Vous devez effacer les propriétés suivantes pour pouvoir définir l'URL de l'instance : proxy Glide, servlet Glide.	
La mise en service de <custom_domain> est toujours en cours. Ce processus peut prendre jusqu'à X heures. Votre administrateur d'instance recevra une notification une fois ce processus terminé.	Une fois que la mise en service d'une instance a commencé pour une URL personnalisée, vous devez attendre la fin du processus avant que l'état ne change.
<custom_domain> est maintenant défini comme nouvelle URL d'instance. <base.service-now.com> est toujours en service, mais toutes les nouvelles URL, par exemple dans les notifications, utiliseront <custom_domain>.	Une seule URL peut être désignée comme URL d'instance. Les autres URL associées à votre instance peuvent être actives, mais seule l'URL d'instance peut utiliser des notifications.
La <custom_domain> URL personnalisée est définie pour être immédiatement supprimée de la configuration d'instance et revenir à <base.service-now.com>. <custom_domain> continue une association à cette instance tant que l'enregistrement CNAME dans votre DNS est défini.	Ce message confirme votre intention de modifier votre URL personnalisée. En acceptant cette confirmation, vous initiez le changement de l'URL vers votre instance. Toute URL figurant sur votre liste de noms de domaine, en tant qu'URL personnalisée, peut être active à moins que vous ne la supprimiez de l'enregistrement CNAME sur votre fournisseur.
Vous ne pouvez pas modifier glide.servlet.uri. Cette propriété est définie par URL personnalisée.	
Vous ne pouvez pas modifier glide.proxy.host. Cette propriété est définie par URL personnalisée.	
L'enregistrement CNAME de <custom_domain> ne pointe pas vers <base.service-now.com>.	La configuration côté fournisseur de l'URL n'est pas correcte. Vérifiez votre configuration sur l'enregistrement CNAME.
Enregistrement CNAME manquant pour <custom_domain>.	L'enregistrement CNAME doit être configuré à partir de votre fournisseur d'URL avant que l'URL personnalisée puisse être définie pour votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sorties d'installation

Les sorties d'installation sont des personnalisations qui quittent Java pour appeler un script avant de revenir à Java.

Remarque :
Les fonctionnalités décrites ici nécessitent le rôle **admin.**

Sorties d'installation disponibles

Accédez à la **Définition du système** > **Sorties d'installation**. Certains noms de sortie d'installation (Login, Logout, ValidatePassword, ExternalAuthentication) sont réservés et ne peuvent pas être modifiés. D'autres sorties d'installation peuvent les remplacer par un script personnalisé qui remplace le script dans la sortie d'installation par défaut.

Les sorties d'installation suivantes sont disponibles dans le système de base :

Sortie de l'installation	Description
Connexion	Utilise une paire nom d'utilisateur/mot de passe et s'authentifie avec l'objet utilisateur
Déconnecter	Dirige l'utilisateur vers la page d'accueil lors de la déconnexion ; peut être remplacé par LogoutRedirect
Déconnexion de la redirection	Dirige l'utilisateur vers une URL spécifiée lors de la déconnexion
Authentification externe	Authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie ; peut être remplacé par DigestSingleSignOn et PGPSingleSignOn
DigestSingleSignOn	S'authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie et déchiffre le chiffrement Digest
PGPSingleSignOn	Authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie et déchiffre le chiffrement PGP
Valider le mot de passe	Actif par défaut, à partir de la Helsinki version ; permet aux clients de définir leur propre validation de mot de passe ; peut être remplacé par ValidatePasswordStronger
ValiderPasswordStronger	Exige que les mots de passe comportent au moins 8 caractères et contiennent un chiffre, une lettre majuscule et une lettre minuscule
GetIntegrationSessionTimeout	Implémente le comportement de délai d'expiration de session d'intégration par défaut.

Modifications de connexion

La modification suivante apportée à la sortie de l'installation de la **connexion** définit la valeur du délai d'expiration de la session de chaque utilisateur à mesure que l'utilisateur se connecte. Dans cet exemple particulier, si le nom d'utilisateur est *administrateur*, la session est définie sur le délai d'expiration de 30 secondes.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    process : function() {
      // the request is passed in as a global
      var userName = request.getParameter("user_name");
      var userPassword = request.getParameter("user_password");

      var authed = GlideUser.authenticate(userName, userPassword);
      if (authed) {
        // ************************************************************
        // customization - if the userName == admin, set the session
        // timeout to be 30 seconds. You can implement your own
        // session timeout algorithm here by checking to see if a user
        // belongs to a certain group or has a certain role.
        // Values of setMaxInactiveInterval exceeding 1440 minutes are
        // treated as one day (1440 minutes).

       if (userName == "admin") {
          request.getSession().setMaxInactiveInterval(30);
        }
        // ************************************************************
        return GlideUser.getUser(userName);
      }

      this.loginFailed();

      return "login.failed";
    },

    loginFailed : function() {
      var message = GlideSysMessage.format("login_invalid");
      var gSession = GlideSession.get();
      gSession.addErrorMessage(message);

      var userName = request.getParameter("user_name");
      EventManager.queue("login.failed", "", userName, "");
    }

}
```

Le délai d'expiration de la session peut également être défini en fonction de l'adresse IP.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

    process : function() {
      // the request is passed in as a global
      var userName = request.getParameter("user_name");
      var userPassword = request.getParameter("user_password");

      var authed = GlideUser.authenticate(userName, userPassword);
      if (authed) {

      // ************************************************************
      // customization - if the user is logging in from a particular IP
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        // range starting with XXX.XXX you can implement your own
        // session timeout algorithm here by checking the login IP
        //
        // Values of setMaxInactiveInterval exceeding 1440 minutes are
        // treated as one day (1440 minutes).

        var clientIP = gs.getSession().getClientIP().toString();

        // if client IP starts with specified range
        if (clientIP.indexOf('XXX.XXX') == 0) {
          // set to 10 hours
          request.getSession().setMaxInactiveInterval(60 * 60 * 10);
        }
        // ************************************************************

          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

Information associée

Authentification basée sur la plage IP

Une façon de sécuriser une application Web consiste à restreindre l'accès en fonction de l'adresse IP.

Vous pouvez bloquer l'accès à une adresse ou à une plage d'adresses spécifique que vous soupçonnez d'appartenir à des personnes malveillantes. L'instance vous permet de contrôler l'accès par adresse IP.

Remarque :
Utilisez la politique de contexte de pré-authentification de l'authentification adaptative (AA) pour appliquer des authentifications basées sur IP et des restrictions pour des options supplémentaires. Pour plus d'informations, consultez Authentification adaptative.

Remarques et limitations :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le système ne vous permettra pas de vous verrouiller, donc si vous essayez d'ajouter une règle telle que votre adresse actuelle serait verrouillée, le système vous avertit et refuse votre insertion.
- Si vous êtes à l'intérieur d'un intranet d'entreprise, soyez très prudent lors de la mise en place de vos règles de propriété intellectuelle. L'adresse IP que vous voyez sur votre propre ordinateur (comme 10.10.10.25) n'a généralement aucun rapport avec l'adresse IP sous laquelle vous apparaîtrez sur Internet. Votre société proxie et/ou NAT votre adresse dans un ensemble prévisible d'adresses sortantes que vous devrez probablement interroger votre équipe réseau.
- Un utilisateur dont l'accès est restreint en fonction d'une règle d'accès obtient une erreur 403 sur son navigateur.
- Les utilisateurs restreints n'utilisent pas de transactions, de sémaphores et ne comptent pas dans les comptes de ressources du serveur.
- Cette fonctionnalité ne remplace ni ne remplace vos règles de contrôle d'accès existantes si, par exemple, vous utilisez un VPN pour notre centre de données. Il s'agit d'une vérification supplémentaire qui doit être effectuée en plus des contrôles d'accès que nous avons pu mettre en place sur votre PIX.
- Les règles d'autorisation remplacent toujours les règles de refus. Donc, si une adresse est à la fois autorisée (par une règle) et refusée (par une deuxième règle), elle est en fait autorisée.
- Les blocs d'astérisques et CIDR ne sont pas pris en charge actuellement.
- En ce qui concerne les adresses proxy transférées, les règles d'autorisation sont appliquées à chaque adresse de la chaîne, puis les règles de refus sont appliquées à chaque adresse de la chaîne si aucune des règles d'autorisation ne correspond.
- L'authentification basée sur la plage IP peut affecter le transfert d'ensembles de mises à jour. Si le contrôle d'accès à l'adresse IP est activé sur l'instance source, ajoutez les adresses IP de tous les nœuds d'application prenant en charge votre instance en tant qu'exceptions.

Remarque :
Pour trouver les informations IP de votre instance, connectez-vous à ServiceNow - Prise en charge de NOW et rechercher l'élément de catalogue **de service Mes informations IP** .

Remarque :
Pour en savoir plus sur les propriétés et `glide.ip.authenticate.strict` qui restreignent l'accès à l'instance `com.snc.ipauthenticator` à des plages IP spécifiques, consultez les rubriques suivantes dans Paramètres de renforcement de la sécurité de l'instance :

Restreindre l'accès aux module d'extension de plages d'adresses IP spécifiques [Mis à jour dans Centre de sécurité 1.3]

Contrôle d'accès à l'adresse IP

Appliquez un contrôle d'accès IP au trafic sortant, au trafic entrant ou au trafic bidirectionnel. Le système ne bloque une adresse IP que si une règle de refus associée existe et qu'aucune règle d'autorisation correspondante n'existe. Par défaut, il n'existe aucune restriction d'accès à votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remarque :
Utilisez la politique de contexte de pré-authentification de l'authentification adaptative (AA) pour appliquer des authentifications basées sur IP et des restrictions pour des options supplémentaires. Pour plus d'informations, consultez Authentification adaptative.

Rôle requis : admin

Avertissement :
Le contrôle d'adresse IP est configuré uniquement pour les adresses IP externes et ne bloque pas les adresses IP internes de ServiceNow.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Contrôle d'accès à l'adresse IP** pour afficher une liste de vos contrôles d'accès IP.
   Vous devrez peut-être activer le module d'extension Authentification basée sur la plage IP [com.snc.ipauthenticator].
2. Renseignez le formulaire.

Remarque :
Pour trouver les informations IP de votre instance, connectez-vous à ServiceNow - Prise en charge de NOW et rechercher l'élément de catalogue **de service Mes informations IP** .

Champ	Description
Type	Type de règle de contrôle d'accès à inclure. ○ *Autoriser* : toute adresse IP de cette plage peut interagir avec cette instance. ○ *Refuser* : toute adresse IP de cette plage ne peut pas interagir avec cette instance, sauf si elle est répertoriée dans une règle d'autorisation. De plus, lorsque vous ajoutez des règles de refus, vous ne pouvez pas refuser votre propre adresse IP publique ou votre instance ne met pas à jour une règle de refus. **Remarque :** Pour prendre en charge la maintenance, les mises à niveau et Service client et assistance, certaines ServiceNow adresses IP internes ne peuvent pas être bloquées par les règles de refus.
Direction	Direction de la règle de contrôle d'accès IP. ○ **Entrant** : autorise ou refuse les transactions entrantes. Il s'agit de transactions initiées depuis l'extérieur de votre instance. ○ **Sortant** : autorise ou refuse les transactions sortantes. Il s'agit de transactions initiées à partir de votre instance. ○ **Bidirectionnel** : autorise ou refuse les transactions entrantes et sortantes.
Actif	Lorsque cette option est sélectionnée, le formulaire est actif.
Description	Description du contrôle d'accès.
Début de plage	Plage de départ d'adresses IP à autoriser ou refuser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ces règles affectent également le transfert des ensembles de mises à jour. Pour vous assurer que le contrôle d'accès à l'adresse IP n'entraîne pas l'échec des ensembles de mises à jour, ajoutez l'instance cible en tant qu'exception.
Fin de plage	Plage de fin d'adresses IP à autoriser ou refuser. **Remarque :** Pour limiter l'accès à des adresses VPN spécifiques uniquement, saisissez une plage de refus comprise entre **0.0.0.0** et **255.255.255.255** dans le champ **de refus** , et saisissez uniquement les plages VPN spécifiques autorisées.

3. Cliquez sur **Envoyer**.

Rechercher les adresses IP refusées

Recherchez les adresses IP refusées dans les fichiers journaux des nœuds de l'instance.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les entrées de journal pour l'adresse IP bloquée apparaissent comme suit : `2015-10-21 18:37:43 (175) http-30 AVERTISSEMENT *** AVERTISSEMENT *** Sécurité restreinte : accès restreint (xx.xx.xxx.xxx non autorisé).`

Remarque :
Les adresses IP refusées sont les fichiers journaux de nœud de l'instance visibles, non visibles dans les journaux système.

Procédure

1. Accédez à la **Tous** > **Journaux système** > **Utilités** > **Navigateur de fichier journal de nœud.**.
2. Parcourez les journaux par critères, tels que la période et le message.
3. Vous pouvez également télécharger des fichiers journaux lorsque vous savez quel journal vous recherchez, en accédant à **Journaux système** > **Utilités** > **Téléchargement du fichier journal de nœud**.

Intégration du protocole LDAP

Une intégration LDAP permet à votre instance d'utiliser votre serveur LDAP existant comme source principale de données utilisateur.

Les administrateurs s'intègrent à un répertoire LDAP (Lightweight Directory Access Protocol) pour rationaliser le processus de connexion de l'utilisateur et automatiser les tâches administratives telles que la création d'utilisateurs et leur affectation de rôles. Une intégration LDAP permet au système d'utiliser votre serveur LDAP existant comme source principale des données utilisateur. En règle générale, une intégration LDAP fait également partie d'une implémentation d'authentification unique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'intégration utilise les informations d'identification du compte de service LDAP pour récupérer le nom distinct (ND) de l'utilisateur à partir du serveur LDAP. Compte tenu de la valeur DN pour l'utilisateur, l'intégration rétablit la liaison avec LDAP en utilisant le ND et le mot de passe de l'utilisateur. Le mot de passe que l'utilisateur entre est entièrement contenu dans la session HTTPS. L'intégration ne stocke jamais les mots de passe LDAP.

L'intégration utilise une connexion en lecture seule qui n'écrit jamais dans le répertoire LDAP. L'intégration interroge uniquement des informations, puis met à jour sa base de données interne en conséquence.

Remarque :
Pour en savoir plus sur la configuration de l'intégration, reportez-vous à la section Configuration de l'intégration LDAP.

Remarque :
Si votre instance utilise une intégration LDAP et que les paramètres Active Directory exigent que les utilisateurs réinitialisent leur mot de passe lors de la connexion, vos utilisateurs ne pourront pas se connecter dans l'instance. L'instance ne peut pas changer le mot de passe Active Directory d'un utilisateur.

Fonctionnalités de l'intégration LDAP

Les fonctionnalités de l'intégration LDAP sont notamment les suivantes.

Actualisation LDAP planifiée

Une analyse planifiée de votre serveur LDAP est généralement exécutée une fois par nuit. Il interroge les attributs de tous les enregistrements utilisateur applicables et les compare avec le compte sur nos serveurs. S'il y a une différence, nous modifions notre enregistrement utilisateur avec l'attribut modifié. La charge placée sur le serveur LDAP pendant l'actualisation dépend du nombre d'enregistrements interrogés et du nombre d'attributs comparés. Nous vous recommandons de programmer l'actualisation en dehors des heures de pointe. Une opération d'actualisation importante peut affecter d'autres opérations planifiées, telles que l'exécution de rapports, et doit être planifiée de manière à minimiser les conflits.

Écouteur LDAP

L'écouteur LDAP est notre version d'une requête persistante (ou recherche persistante). Nous émettons une requête permanente pour les modifications apportées à votre serveur LDAP et sommes constamment à l'écoute d'une réponse. En supposant que votre serveur prend en charge une recherche persistante, toutes les modifications apportées à l'un de vos comptes LDAP applicables sont renvoyées à l'écouteur LDAP et envoyées à votre instance dans un délai d'environ 10 secondes. Il s'agit d'un outil extrêmement utile, qui nous permet d'avoir une copie en temps quasi réel des détails du compte de vos utilisateurs, sans avoir à attendre la prochaine actualisation planifiée.

Connexion LDAP à la demande

Une fois l'intégration LDAP établie, l'instance peut autoriser de nouveaux utilisateurs à se connecter au système, même s'ils n'ont pas encore de compte sur l'instance. Lorsqu'un nouvel utilisateur tente de se connecter à l'instance, l'intégration vérifie si cet utilisateur a un compte dans l'instance. Si l'intégration ne trouve pas de compte d'utilisateur existant, elle interroge automatiquement le serveur LDAP pour obtenir le nom d'utilisateur saisi. Si un compte LDAP correspondant est trouvé, l'intégration tente de s'authentifier avec le mot de passe que l'utilisateur a entré. Si le mot de passe est valide, l'instance crée un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

compte pour l'utilisateur, remplit le compte avec toutes les informations LDAP applicables et connecte l'utilisateur à l'instance.

La connexion à la demande utilise la carte de transformation d'importation d'utilisateur LDAP. Pour en savoir plus sur les exigences relatives aux cartes de transformation, reportez-vous à la section Cartes de transformation LDAP.

Remplissage des données LDAP

> **Remarque :**
> La fonctionnalité décrite dans cette intégration n'est pas disponible par défaut. Cette intégration implique une personnalisation post-déploiement effectuée par un administrateur expérimenté ou par ServiceNow des consultants en services professionnels.

Une intégration aux serveurs LDAP vous permet de renseigner rapidement et facilement la base de données de l'instance avec des enregistrements utilisateur provenant de la base de données LDAP existante. Pour éviter les incohérences de données, vous pouvez créer, ignorer ou ignorer les enregistrements LDAP entrants.

Vous pouvez également limiter les données importées par l'intégration en spécifiant des attributs LDAP, important ainsi uniquement les données que vous souhaitez exposer à une instance. En règle générale, les attributs LDAP que vous spécifiez font partie de la carte de transformation d'intégration. Si vous ne spécifiez aucun attribut LDAP, l'intégration importe tous les attributs d'objet disponibles à partir du serveur LDAP. L'instance stocke les données LDAP importées dans des tables de jeux d'importation temporaires. Ainsi, plus vous importez d'attributs, plus le temps d'importation est long. Pour plus d'informations, consultez Spécifier les attributs LDAP.

Authentification LDAP

Utilisez l'authentification LDAP pour accéder à l'application à l'aide d'informations d'identification LDAP.

Lorsqu'un utilisateur saisit les informations d'identification réseau dans la page de connexion :

1. L'instance transmet les informations d'identification à un serveur LDAP pour trouver l'instance.
2. Avec les NDR, il valide la chaîne DN de l'utilisateur. Elle valide uniquement si au moins une des configurations d'unité organisationnelle LDAP avec `table=sys_user` a un NDR configuré.
3. Le serveur LDAP répond par un message autorisé ou non autorisé que le système utilise pour déterminer si l'accès doit être accordé.

En s'authentifiant sur votre serveur LDAP, les utilisateurs accèdent à la plateforme avec les mêmes informations d'identification que celles qu'ils utilisent pour les autres ressources internes sur votre domaine réseau. Vous pouvez également réutiliser les politiques de mot de passe et de sécurité existantes déjà en place. Par exemple, le serveur LDAP peut déjà avoir des politiques de verrouillage de compte et d'expiration de mot de passe.

Lorsque vous activez LDAP, le système met à jour les enregistrements utilisateur avec ces champs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mises à jour d'enregistrements d'utilisateurs LDAP

Champ	Description
Source	Détermine si LDAP est utilisé ou non pour valider un utilisateur. Si la source commence par ldap, l'utilisateur est validé via LDAP. Si la source ne commence pas par ldap, le mot de passe sur l'enregistrement utilisateur est utilisé pour valider l'utilisateur lors de la connexion.
Serveur LDAP	Identifie quel serveur LDAP authentifie l'utilisateur en présence de plusieurs serveurs LDAP.

Remarque :
Le système ne prend pas en charge l'authentification par mot de passe LDAP via un serveur MID. Une instance doit pouvoir se connecter directement à un serveur LDAP pour prendre en charge l'authentification par mot de passe.

Comprendre l'intégration LDAP

Une intégration LDAP permet à votre instance d'utiliser votre serveur LDAP existant comme source principale de données utilisateur.

Prérequis de l'intégration LDAP

- Le serveur des services de répertoire doit être compatible LDAP v3
- L'accès au réseau entrant via le pare-feu doit être autorisé (vers le serveur LDAP)
- Adresse IP externe ou nom du serveur LDAP
- Informations d'identification de l'utilisateur avec accès en lecture seule
- Pour LDAPS, un certificat PKI

Synchronisation de l'intégration LDAP

Les intégrations LDAP se font généralement avant la mise en service de l'instance, mais peuvent être intégrées à tout moment.

Intégrité des données du serveur LDAP

Certains utilisateurs s'inquiètent du fait qu'un tiers (l'instance dans ce cas) apporte des modifications (écriture) à votre serveur LDAP. Dans une intégration LDAP, votre instance n'écrit pas dans le répertoire LDAP interne. L'instance interroge des informations et met à jour sa base de données en conséquence.

Aucune modification n'est apportée au serveur LDAP interne par l'instance. Le compte de service est en lecture seule.

La plupart des changements (y compris les ajouts) apportés à votre serveur LDAP sont disponibles en quelques secondes pour l'instance, en fonction du nombre de composants de l'intégration LDAP complète en place.

Pour maintenir les enregistrements LDAP synchronisés, planifiez une analyse périodique du serveur LDAP pour détecter les changements.

L'instance ne synchronise pas les enregistrements de département. Les utilisateurs et les appartenances aux groupes sont tenus à jour par le mécanisme d'écoute LDAP et une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

navigation LDAP quotidienne complète, mais l'instance ne supprime aucune de ces entrées une fois qu'elles ont disparu de LDAP.

Si une entrée devait être supprimée, tout l'historique serait également supprimé, et toute référence à celle-ci serait effacée ou supprimée. Les éléments de configuration (CI), les accords SLA, les licences de logiciels, les bons de commande et les entrées de Service Catalog ont tous une référence au département, et si le département est supprimé, ces références sont effacées. Il y a beaucoup de références aux utilisateurs, et donc supprimer un utilisateur perdrait tout l'historique de ce qu'il a fait. Actuellement, la décision de supprimer ou non est prise par nos clients.

Sécurité

La connexion est établie à partir d'une seule machine à l'aide d'une adresse IP fixe via un port spécifique sur votre pare-feu. L'authentification est effectuée avec un compte LDAP en lecture seule de votre choix. Vous pouvez utiliser LDAP standard, ou charger la face publique d'un certificat SSL installé sur votre annuaire, auquel cas nous pouvons utiliser LDAPS. Pour ajouter une autre couche de sécurité, nous offrons également l'option d'un tunnel VPN IPSEC point à point. Contactez votre chargé de clientèle pour plus de détails et de tarification.

Connexions LDAP sécurisées

Connexion	Description
Serveur MID	Pour protéger votre serveur LDAP du trafic réseau externe, installez un serveur MID sur le réseau local et configurez le système pour qu'il communique avec le serveur MID via un canal sécurisé.
LDAPS	Pour établir une connexion LDAPS chiffrée, chargez le côté public du certificat SSL de votre serveur LDAP. L'intégration utilise le certificat pour chiffrer toutes les communications entre le serveur LDAP et l'instance.
VPN	Pour sécuriser le serveur LDAP avec un tunnel VPN IPSEC point à point chiffré, contactez votre chargé de clientèle pour plus de détails et de tarifs.

Un autre aspect de la sécurité à prendre en compte est les données partagées dans une intégration LDAP. Pour limiter les données exposées à votre instance, spécifiez des attributs dans votre carte de transformation. Pour plus d'informations, consultez Cartes de transformation LDAP.

Importation de données LDAP dans l'instance

Il est recommandé de définir les attributs pour importer uniquement les données requises. Les attributs définis sont mappés dans la base de données de l'utilisateur d'instance.

Nous ne pouvons pas répondre à la question de savoir quels attributs spécifiques sont nécessaires, car cela est déterminé par la portée du projet et les exigences de l'entreprise.

Types de serveurs LDAP pris en charge

L'instance s'est intégrée avec succès à Microsoft Active Directory, Novell, Domino (Lotus Notes) et Open LDAP. Nous utilisons JNDI pour nous interfacer avec le serveur LDAP. Tant que votre serveur LDAP est conforme à la norme LDAP v3, l'intégration est réussie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification unique LDAP

Outre la fonctionnalité de remplissage de données fournie avec l'importation LDAP, vous pouvez utiliser la fonctionnalité d'authentification externe prise en charge par l'application pour empêcher vos utilisateurs d'avoir à se connecter à chaque fois.

Plusieurs domaines LDAP

La méthode recommandée pour gérer plusieurs domaines consiste à créer un enregistrement de serveur LDAP distinct pour chaque domaine. Chaque enregistrement de serveur LDAP doit pointer vers un contrôleur de domaine pour ce domaine. Cela signifie que le réseau local doit autoriser les connexions à chacun des contrôleurs de domaine.

Après l'extension à plusieurs domaines réseau, il est essentiel d'identifier les attributs LDAP uniques pour les noms d'utilisateur de l'application et d'importer les valeurs de fusion. Un attribut de fusion unique commun pour Active Directory est objectSid. Les noms d'utilisateur uniques peuvent varier en fonction de la conception des données LDAP. Les attributs communs sont email ou userPrincipalName.

Gestion des limites de requête

Par défaut, Active Directory 2000/2003 dispose d'une limite de requêtes LDAP (maxPageSize) de 1 000 objets pour éviter les charges excessives et les attaques par déni de service. Nous avons deux méthodes pour faire face à cette limite.

La méthode par défaut consiste à diviser la requête pour renvoyer moins de 1 000 objets à la fois. Par exemple, interrogez uniquement les objets commençant par la lettre « a », puis les objets « b ». La méthode la plus efficace pour les grands environnements est d'activer la pagination. La pagination est prise en charge par défaut sur tous les serveurs Microsoft Active Directory. Il divise automatiquement les résultats en plusieurs ensembles de résultats, de sorte que nous n'avons pas à diviser la requête en plusieurs demandes.

Type de requête LDAP

Si un mot de passe LDAP est fourni, une « liaison simple » est effectuée. Si aucun mot de passe LDAP n'est fourni, la valeur « aucun » est utilisée, auquel cas le serveur LDAP doit autoriser la connexion anonyme.

Authentification LDAP

Nous utilisons les informations d'identification de compte de service fournies pour LDAP afin de récupérer le ND de l'utilisateur à partir du serveur LDAP. Compte tenu de la valeur DN de l'utilisateur, nous rétablissons la liaison avec LDAP compte tenu du DN de l'utilisateur et du mot de passe fourni.

Stockage des mots de passe

Le mot de passe que l'utilisateur entre est entièrement contenu dans sa session HTTPS. Nous ne stockons ce mot de passe nulle part.

Configuration de l'authentification LDAP

Ces champs de l'enregistrement utilisateur se rapportent au LDAP :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Source** : le champ Source identifie si un utilisateur est validé ou non à l'aide de LDAP. Si le champ source commence par « ldap », l'utilisateur est validé via LDAP. Si le champ Source ne commence pas par « ldap », le mot de passe figurant sur l'enregistrement utilisateur est utilisé pour valider l'utilisateur lors de la connexion.
- **Serveur LDAP** : l'instance prend en charge plusieurs serveurs LDAP, de sorte que le champ Serveur LDAP détermine quel serveur doit être utilisé pour authentifier l'utilisateur.

Exigences relatives à l'intégration LDAP

Passez en revue les exigences pour l'intégration LDAP, qui incluent un certificat PKI et un serveur de services d'annuaire compatible LDAP.

L'intégration LDAP nécessite :

- Un serveur de services d'annuaire compatible LDAP v3
  - Permet l'accès au réseau entrant via le pare-feu (vers le serveur LDAP)
  - (Facultatif) Accepte la connexion anonyme
  - (Facultatif) Prend en charge la pagination pour les requêtes LDAP volumineuses
- Adresse IP externe ou nom de domaine complet du serveur LDAP. Vous pouvez également utiliser un serveur MID.
- Compte LDAP en lecture seule de votre choix
- Pour plusieurs domaines, accès au réseau pour chaque contrôleur de domaine
- Pour LDAPS, un certificat PKI
- Pour l'écouteur LDAP, un serveur Microsoft Active Directory qui prend en charge les requêtes persistantes (ADNotify)

Serveurs LDAP pris en charge

En utilisant *JNDI* comme interface avec le serveur LDAP, l'instance s'est intégrée avec succès aux serveurs suivants :

- Microsoft Active Directory
- Novell
- Domino (Lotus Notes)
- Ouvrir LDAP

Limites des requêtes LDAP

Par défaut, Active Directory 2000/2003 dispose d'une limite de requêtes LDAP (maxPageSize) de 1 000 objets pour éviter les charges excessives et les attaques par déni de service. Le système dispose de deux méthodes pour faire face à cette limite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La méthode par défaut consiste à diviser la requête pour renvoyer moins de 1 000 objets à la fois. Par exemple, interrogez uniquement les objets commençant par la lettre a, puis interrogez les objets b.
- La méthode la plus efficace pour les environnements volumineux consiste à activer la pagination, qui est prise en charge par défaut sur tous les serveurs Microsoft Active Directory. La pagination divise automatiquement les résultats en plusieurs ensembles de résultats afin que l'intégration n'ait pas à diviser la requête en plusieurs demandes.

Configuration de l'intégration LDAP

Les administrateurs peuvent activer l'intégration LDAP pour permettre l'authentification des utilisateurs à partir de l'annuaire LDAP de leur entreprise.

LDAP utilise généralement l'un de ces types de canaux de communication.

Canaux de communication LDAP

Connexion	Description	Prise en charge de l'importation LDAP ?	Prise en charge de l'authentification LDAP ?
Connexion au serveur MID	Communique via HTTP sur le port 80 par défaut. Ce canal de communication ne nécessite pas de certificat. La connexion entre le serveur MID et l'instance se fait via HTTPS (port 443). Vous pouvez utiliser le serveur MID pour importer des données via LDAP, mais vous ne pouvez pas utiliser le serveur MID pour l'authentification LDAP. Poursuivez avec la définition du serveur LDAP.	Oui	Non
Intégration LDAP standard	Communique par défaut via TCP sur le port 389. Ce canal de communication ne nécessite pas de certificat. Poursuivez avec la définition du serveur LDAP.	Oui	Oui
Intégration LDAP chiffrée SSL (LDAPS)	Communique par défaut via TCP sur le port 636. Ce canal de communication nécessite un certificat. Procédez à pour Installer le certificat SSL LDAP X.509 obtenir et charger le certificat.	Oui	Oui
Connexion VPN	Communique via un tunnel IPSEC. Achetez ou créez un tunnel IPSEC sur votre réseau local. Poursuivez avec la définition du serveur LDAP.	Oui	Oui

Si vous utilisez un serveur MID, le serveur MID se connecte à l'instance et le serveur MID se connecte également au serveur LDAP. Dans les deux cas, le MID Server initie la connexion :

1. Tout d'abord, le serveur MID se connecte au serveur LDAP via LDAP sur le port 389.
2. Ensuite, le serveur MID établit une connexion chiffrée HTTPS à l'instance sur le port 443 pour transmettre les données à l'instance.

Pour plus d'informations sur les VPN, les serveurs MID et LDAP, consultez Vous n'avez pas besoin d'un VPN Partie II sur la communauté.

Installer le certificat SSL LDAP X.509

Vous pouvez installer un certificat X.509 pour votre intégration LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Procédure

1. Achetez ou générez un certificat SSL sur votre serveur LDAP.
2. Accédez à la **LDAP** > **Certificat** et cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire :

Champ	Description
Nom	Le nom du certificat.
Notification d'échéance	Sélectionnez cette option pour envoyer une notification aux utilisateurs sélectionnés dans le champ **Notification à l'expiration** . Cette option est activée par défaut.
Notification à l'expiration	Sélectionnez les utilisateurs pour relancer la notification concernant l'expiration du certificat. Si aucun utilisateur n'est sélectionné, l'utilisateur connecté est ajouté par défaut, ainsi que les deux derniers utilisateurs connectés disposant du rôle d'administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l'expiration à l'origine de l'envoi de la notification par l'instance. Saisissez une valeur d'au moins 20. Cette valeur est définie sur 20 pour les instances mises à niveau vers Istanbul et les versions ultérieures, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher indiquant que ce certificat est actif.
Format	Le format du certificat.
Type	Le conteneur du certificat. L'instance reconnaît les certificats des magasins de clés de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Début de validité	L'instance ajoute automatiquement la date de début de validité du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Date d'expiration	L'instance ajoute automatiquement la date d'expiration du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Échéance en jours	Nombre calculé de jours jusqu'à l'expiration.
Description brève	Description du certificat.
Émetteur	L'instance ajoute automatiquement l'émetteur du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Objet	L'instance ajoute automatiquement le certificat soumis à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Entrez la valeur du certificat X509.

Remarque :
L'intégration ne signe pas actuellement le certificat dans les communications entre l'instance et l'IdP.

4. Cliquez sur **Enregistrer**.

Que faire ensuite

Cliquez sur **Valider les banques/certificats** pour tester le magasin de confiance et le certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

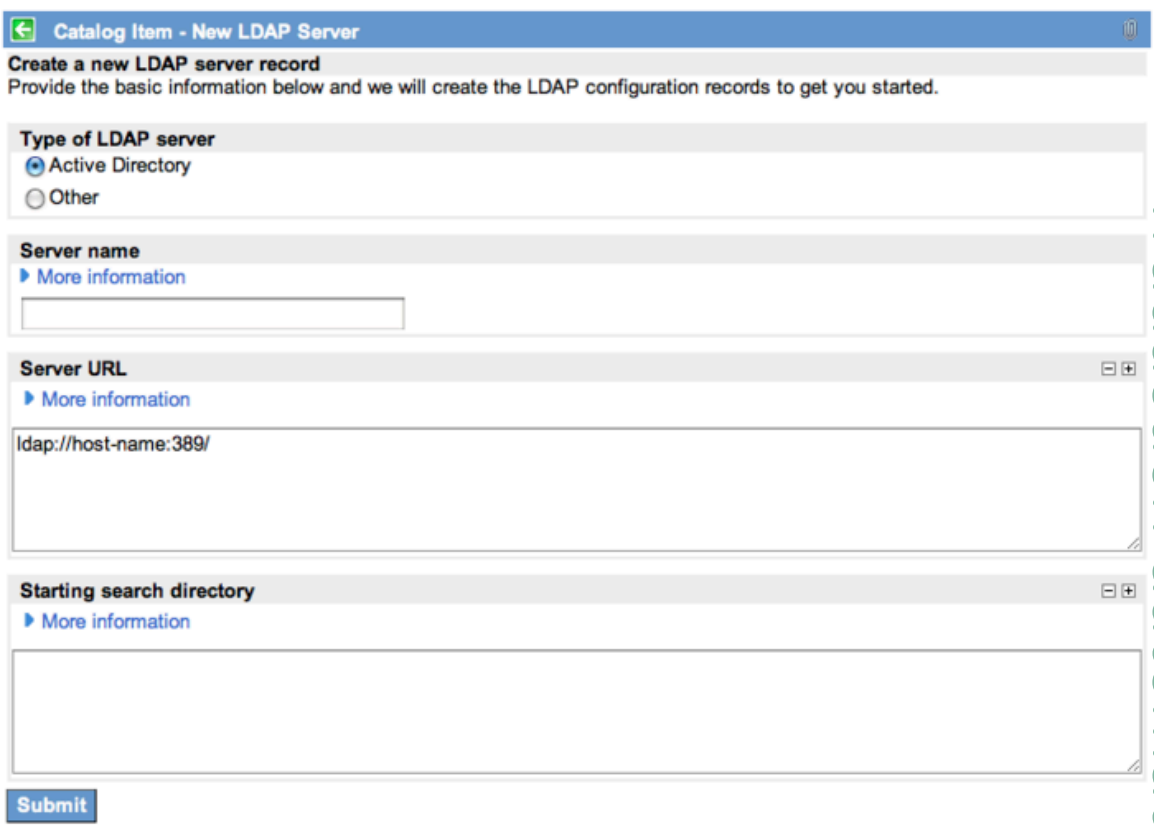
Définir un serveur LDAP

Créez un nouvel enregistrement de serveur LDAP dans l'instance.

Avant de commencer
Rôle requis : admin.

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Créer un serveur**.
2. Renseignez les champs de formulaire.



Dans le champ **URL du serveur** , les URL valides de tous les serveurs apparaissent séparées par un espace. Les serveurs sont d'abord classés par statut opérationnel, les serveurs répertoriés **en** premier, puis classés par la valeur **d'ordre** que vous spécifiez. Le premier serveur répertorié est le serveur LDAP principal. Les autres sont des serveurs redondants.

Remarque :
Il y a un léger délai entre le changement de l'état opérationnel réel et l'affichage.

Vous pouvez également ajouter un serveur LDAP redondant en accédant à un enregistrement de serveur LDAP existant et en insérant une ligne dans la liste incorporée URL du serveur LDAP.

3. Cliquez sur **Envoyer**.

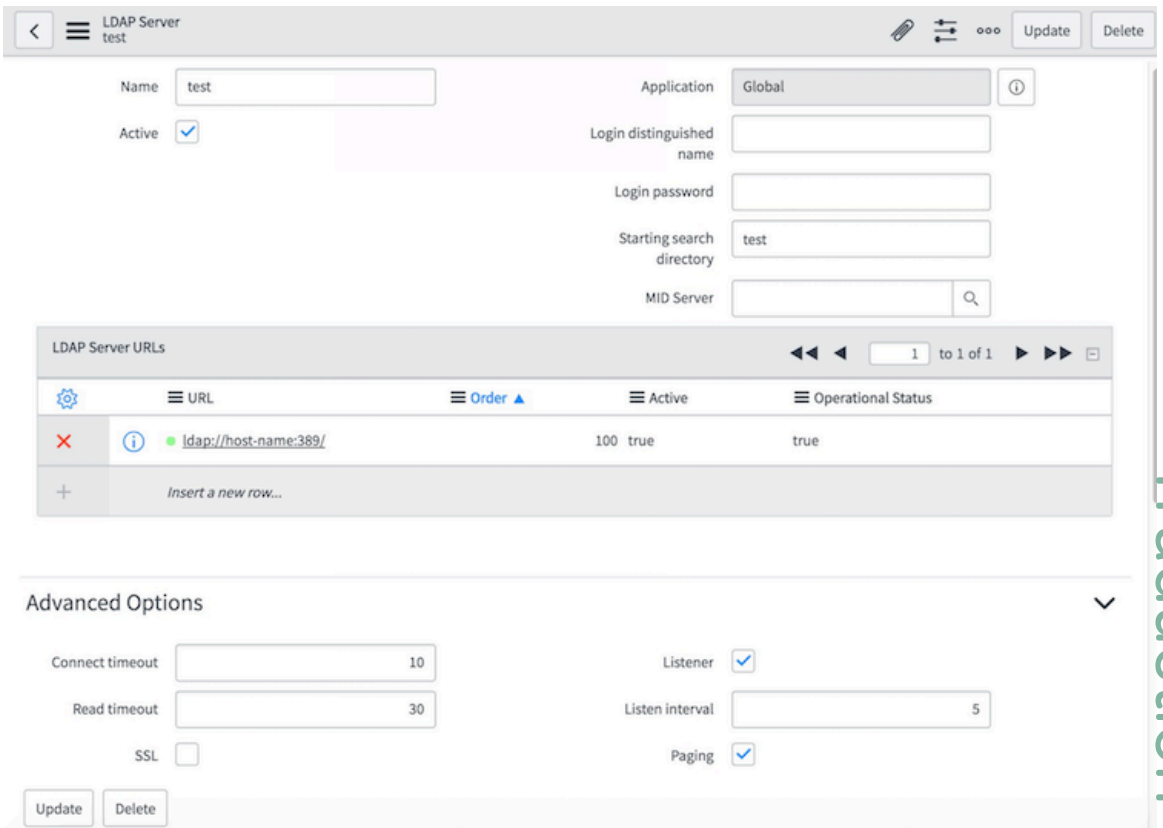
Remarque :
Vous pouvez également modifier un enregistrement de serveur LDAP existant en accédant à **Système LDAP** > **Serveurs LDAP** et apporter les changements nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Apportez des modifications aux champs si nécessaire.

Formulaire du serveur LDAP



Champ	Description
Nom	Entrez le nom du serveur.
Actif	Cochez cette case si le serveur est actif.
URL des serveurs LDAP	Entrez les URL des serveurs LDAP principal et des serveurs LDAP de secours. Les serveurs sont d'abord classés par statut opérationnel, les serveurs répertoriés en premier, puis classés par la valeur d'ordre que vous spécifiez. Le premier serveur répertorié est le serveur LDAP principal. Les autres sont des serveurs redondants.
URL serveur	Entrez l'URL du serveur. Configurez le formulaire pour ajouter ce champ si nécessaire. Il s'agit d'un champ calculé en lecture seule qui affiche la liste des serveurs LDAP que vous pouvez également voir dans le champ **URL des serveurs LDAP** , séparés par un espace et classés par statut opérationnel et valeurs d'ordre des URL.
Nom de connexion distinct	Entrez le nom unique (DN) de l'utilisateur authentifiant la connexion LDAP. Pour accéder à un serveur d'annuaire LDAP, le nom d'utilisateur doit être au format de nom distinct complet : servicenow@service-now.com
Mot de passe de connexion	Entrez le mot de passe du serveur.
Répertoire de recherche de départ	Entrez le nom distinct relatif (NDR) du répertoire de recherche par défaut. Toutes les requêtes adressées à ce serveur LDAP commenceront à partir de ce NDR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveur MID	Sélectionnez le serveur MID que vous souhaitez utiliser pour vous connecter au serveur LDAP. L'utilisation d'un serveur MID pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il élimine également le besoin d'établir un tunnel VPN entre votre serveur LDAP et ServiceNow les centres de données. **Remarque :** ◦ L'utilisateur du Serveur MID doit disposer du rôle user_admin afin de pouvoir lire les enregistrements de configuration du serveur LDAP. ◦ Les éléments suivants ne sont pas disponibles avec le Serveur MID : ▪ Authentification LDAP ▪ Connexion SSL
Délai de Connexion	Si un serveur MID est configuré, la connexion expire au bout de 10 secondes, quel que soit ce paramètre. Ce paramètre est codé en dur et ne peut pas être modifié.
Délai d'expiration de lecture	Spécifiez le nombre de secondes dont dispose l'intégration pour lire les données LDAP. L'intégration arrête la lecture des données LDAP après que la connexion a dépassé le délai de lecture. Si vous activez une connexion SSL, vous pouvez également définir une valeur de délai de lecture avec la`com.glide.ssl.read.timeout`propriété système. Si vous entrez des valeurs de délai d'expiration pour ce champ et pour la propriété système, la valeur de délai d'expiration la plus basse est prioritaire.
SSL	Cochez cette case pour exiger du serveur LDAP qu'il établisse une connexion chiffrée SSL. Si vous avez sélectionné un serveur MID, ce champ n'est pas disponible. Si vous utilisez une intégration LDAPS et que le port SSL par défaut est 636, aucune autre configuration n'est nécessaire ; SSL est automatiquement activé. Si l'intégration LDAPS utilise un autre port SSL, définissez les autres propriétés de connexion SSL. **Remarque :** Assurez-vous qu'un administrateur réseau configure le pare-feu local pour permettre au serveur d'applications d'accéder au serveur LDAP. Si le serveur LDAP est situé dans un réseau interne, le pare-feu transmet (ou NAT) l'adresse IP du serveur d'applications via le pare-feu sur le port approprié.
Écouteur	Cochez cette case pour permettre à l'intégration d'interroger Microsoft périodiquement les serveurs Active Directory ou LDAP qui prennent en charge le contrôle persistant des demandes de recherche. En outre, si vous avez sélectionné un serveur MID, la fonctionnalité d'écoute est disponible pour ce serveur MID. Consultez Activer un écouteur LDAP et définir les propriétés système pour plus d'informations.
Intervalle d'écoute (valeur	Spécifiez la valeur du délai d'expiration de l'écouteur en nombre de minutes pendant lesquelles l'intégration écoute les données LDAP à chaque connexion. L'intégration arrête l'écoute des données LDAP après que la connexion dépasse l'intervalle d'écoute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
de délai d’expiration)	
Pagination	Cochez cette case pour que le serveur LDAP divise les données d’attributs LDAP en plusieurs jeux de résultats plutôt que d’envoyer plusieurs requêtes.

Remarque :
Si vous fournissez un mot de passe LDAP, l’intégration effectue une opération de liaison simple. Si vous ne fournissez pas de mot de passe LDAP, le serveur LDAP doit autoriser la connexion anonyme, sinon l’intégration ne peut pas se lier au serveur LDAP.

Résultats

Lorsqu’un enregistrement du serveur LDAP est défini sur actif, le système teste automatiquement chaque connexion pour le valider.
Les validations comprennent :

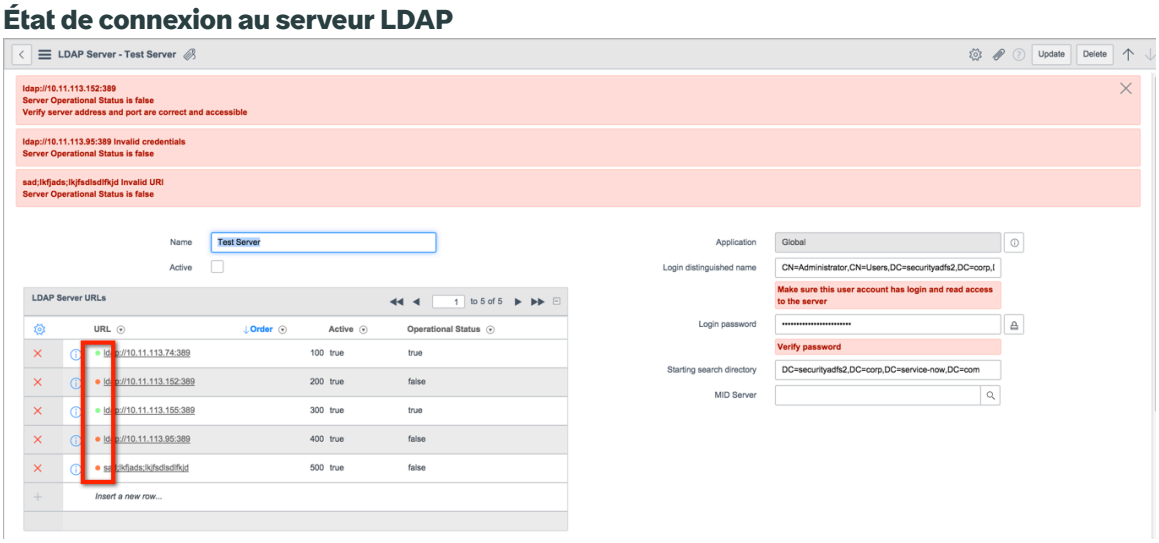
- Le serveur LDAP est accessible à l’URL et au port fournis
- L’URL du serveur LDAP est correctement formatée
- Les informations d’identification de connexion sont valides

À partir de la version Fuji, le système affiche des points colorés à côté de chaque URL de serveur :

Icônes de connexion au serveur LDAP

Couleur	Description
Vert	Le serveur s’il est actif et opérationnel.
Gris	Le serveur n’est ni actif ni opérationnel.
Rouge	Le serveur est actif mais non opérationnel.

État de connexion au serveur LDAP



Activer un écouteur LDAP et définir les propriétés système

L’activation d’un écouteur est facultative. Si cette fonction est activée, un écouteur avertit le système de traiter les enregistrements LDAP peu de temps après une mise à jour du serveur LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Un *écouteur* est un processus dédié qui recherche périodiquement des modifications sur le serveur LDAP.

L'écouteur peut être déployé sur un serveur Microsoft Active Directory qui prend en charge les requêtes persistantes (ADNotify) ou sur un serveur LDAP qui prend en charge le contrôle persistant des demandes de recherche (avec OID 2.16.840.1.113730.3.4.3).

Si le serveur LDAP prend en charge une recherche persistante, l'écouteur LDAP reconnaît toutes les modifications apportées à l'utilisateur et au groupe sur l'un des comptes LDAP applicables et les transmet à votre instance dans un délai d'environ 10 secondes. Cela permet à l'instance de disposer d'une copie en temps quasi réel des détails du compte de vos utilisateurs sans avoir à attendre la prochaine actualisation planifiée. L'écouteur LDAP ne peut synchroniser que les objets mappés aux tables Utilisateur [sys_users] et Groupe [sys_user_group].

Remarque :
Si un utilisateur est ajouté via l'écouteur, mais qu'il ne répond pas aux exigences définies par le filtre UO, l'instance ignore l'enregistrement sur le serveur LDAP. S'il répond aux critères, l'utilisateur est ajouté à l'instance.

Pour activer un écouteur :

Procédure
1. Accédez à la **Tous** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Cochez la case **Écouteur** .
4. Cliquez sur **Mettre à jour**.

Remarque :
Le système importe uniquement les enregistrements utilisateur qui correspondent au filtre LDAP UO. Les enregistrements d'utilisateurs entrants qui ne répondent pas aux exigences de filtrage sont marqués comme non valides et ignorés par l'importation. Les administrateurs peuvent activer la journalisation LDAP détaillée pour déterminer si les enregistrements entrants ne correspondent pas au filtre LDAP UO.

5. **Facultatif :** Accédez à la table Propriétés système [sys_properties] et définissez les propriétés système de l'écouteur LDAP.

Propriétés de l'écouteur LDAP

Propriété	Description
glide.ldap.listener.use_background_transaction	Si la valeur est vrai, l'écouteur LDAP est démarré en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction d'ar plan, la règle de quota Démarrage/arrêt de l'écouteur LDAP peut annuler la transaction une fois la durée maximale atteinte, 5 minutes par défaut. C comportement empêche un écouteur LDAP d'attendre indéfiniment.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : Cette propriété s'applique uniquement aux connexions LDAP qui n'utilisent pas de serveur MID. Utilisez cette propriété `glide.ldap.listener.mid.use_background_transac` pour contrôler le comportement des connexions LDAP qui passent pa Serveur MID. ○ Type : true | false ○ Valeur par défaut : faux ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.use_background_transaction	Si la valeur est vrai, l'écouteur LDAP est démarré en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction d'ar plan, la règle de quota Démarrage/arrêt de l'écouteur LDAP Transaction M peut annuler la transaction une fois la durée maximale atteinte, 5 minutes défaut. Ce comportement empêche un écouteur LDAP d'attendre indéfini **Remarque :** Cette propriété s'applique uniquement aux connexions LDAP qui utilisent un serveur MID. Utilisez cette propriété `glide.ldap.listener.use_background_transaction` contrôler le comportement des connexions LDAP qui ne passent pas un serveur MID. ○ Type : true | false ○ Valeur par défaut : faux ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.one_listener	Si la valeur est vrai, un seul message de file d'attente ECC est créé pour démarrer ou arrêter l'écouteur LDAP via un serveur MID. Si la valeur est sur false, plusieurs messages de file d'attente ECC peuvent être créés, ce entraîne la création de plusieurs threads pour démarrer ou arrêter l'écouteu LDAP. ○ Type : true | false ○ Valeur par défaut : true ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]

Traduction automatique

Spécifier les attributs LDAP

Spécifiez les attributs inclus dans les requêtes de serveur LDAP à l'aide du champ **Attributs** du serveur LDAP. Cela peut améliorer les performances ainsi que la sécurité.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Par défaut, le système charge tous les attributs de chaque objet qu'il est autorisé à lire à partir de votre serveur LDAP. À l'aide du champ **Attributs** , vous pouvez spécifier et ainsi

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

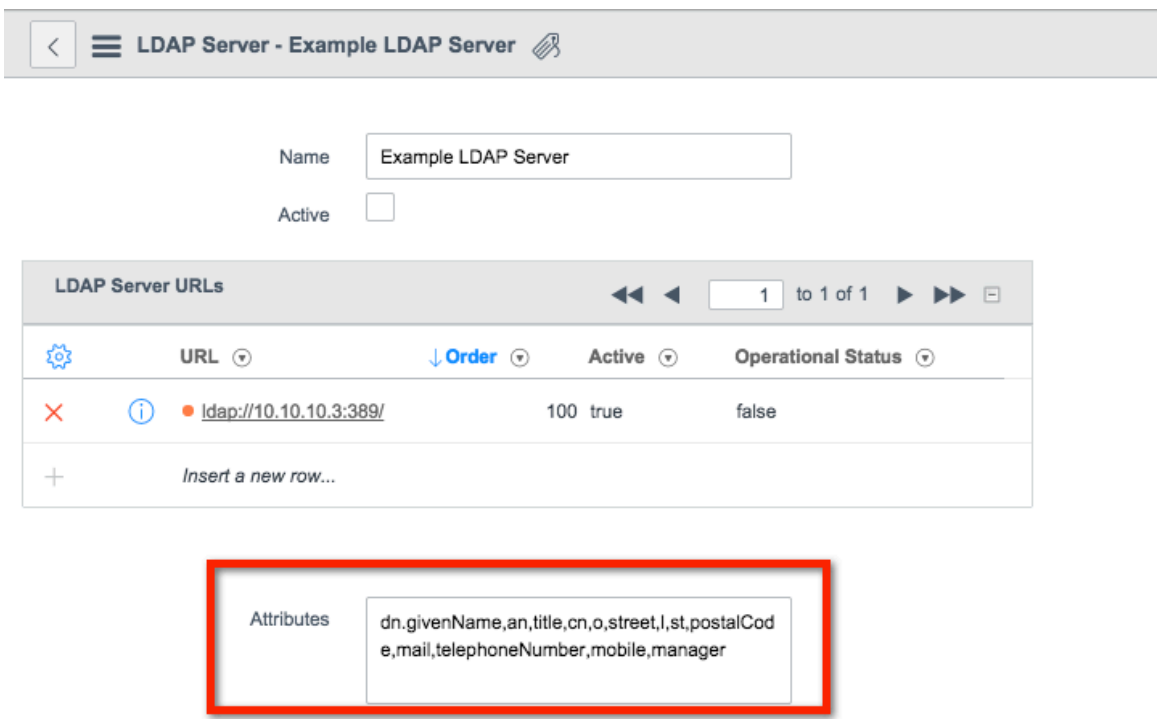
limiter les attributs renvoyés par la requête LDAP. L'utilisation de cette approche pour les importations LDAP volumineuses peut améliorer considérablement la vitesse de ces importations.

Procédure

Définissez explicitement les attributs dans la mesure du possible.

S'il existe des informations que vous ne souhaitez pas voir exposées à l'instance, excluez l'attribut. Si vous ne spécifiez pas d'attributs de serveur LDAP, les transactions utilisateur peuvent se bloquer pendant de longues périodes lorsque de nouveaux attributs sont ajoutés à un objet de serveur LDAP, car le système est occupé à charger les données à partir des nouveaux attributs.

Remarque :
Pour utiliser les scripts de recherche de gestionnaire décrits dans Sélectionner ou créer une carte de transformation pour les données LDAP, spécifiez **le gestionnaire** et le **nom unique** dans le champ **Attributs** . Aucun des deux attributs n'est requis pour faire partie d'une carte de transformation.



Tester une connexion LDAP

L'instance teste automatiquement la connexion chaque fois qu'un utilisateur ouvre le formulaire du serveur LDAP. Vous pouvez également tester manuellement la connexion au serveur LDAP à partir du formulaire du serveur LDAP.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Par défaut, des messages d'erreur s'affichent sur le formulaire du serveur LDAP en cas de problème de connexion au serveur LDAP.

Remarque :
Les employés peuvent également vérifier la connectivité entre l'instance et le serveur LDAP. Contactez l'assistance technique pour obtenir de l'aide lors de la vérification de la connectivité LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour tester manuellement une connexion :

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à tester.
3. Sous **Liens connexes**, cliquez sur **Test de la connexion**.
4. Sous **Liens connexes**, cliquez sur **Parcourir** pour vérifier que la structure de répertoire LDAP appropriée est visible pour le système.
5. **Facultatif :** Si la connexion a réussi, cliquez sur **Parcourir** pour afficher la structure du répertoire LDAP source visible par l'instance.

Remarque :
Les champs **Filtre** et **NDR** à gauche de la fenêtre Parcourir sont ignorés lorsque vous utilisez le champ de recherche à droite.

Résultats
L'instance modifie l'état opérationnel des serveurs LDAP en fonction du résultat du test de connexion.

- Si votre instance établit une connexion à un serveur dont la valeur **d'état opérationnel** est **indisponible**, la valeur d'état **opérationnel** est automatiquement changée en **actif**. Cette fonctionnalité est prise en charge pour les tests de connexion automatiques et manuels.
- Si une connexion ne peut pas être établie avec un serveur dont la valeur **d'état opérationnel** est **activée**, la valeur **d'état opérationnel** est automatiquement changée en **indisponible**. Cette fonctionnalité est prise en charge uniquement pour les tests de connexion automatiques, et non pour les tests manuels.

Définir des unités organisationnelles LDAP

Une définition d'unité organisationnelle (OU) spécifie les répertoires sources LDAP disponibles pour l'intégration.

Avant de commencer
Rôle requis : admin.

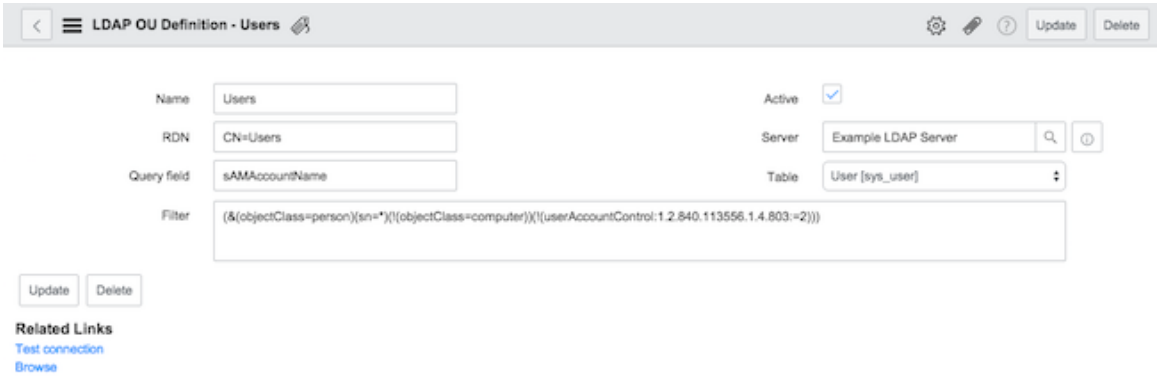
Pourquoi et quand exécuter cette tâche
Les définitions d'unités organisationnelles peuvent contenir des emplacements, des personnes ou des groupes d'utilisateurs. Chaque définition de serveur LDAP contient deux exemples de définitions d'unités organisationnelles : l'une pour l'importation de groupes dans le système et l'autre pour les utilisateurs.

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Dans la liste connexe **Définitions d'unités organisationnelles LDAP** , sélectionnez l'exemple de définition d'unité organisationnelle **Groupes** ou **Utilisateurs** .
4. Remplissez le formulaire Définition LDAP OU (voir table).
5. Cliquez sur **Mettre à jour**.
   Le système teste automatiquement la connexion au serveur LDAP.
6. Sous **Liens connexes**, cliquez sur **Parcourir** pour afficher les enregistrements de répertoire LDAP renvoyés par la définition d'UO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Formulaire de définition d'une unité organisationnelle

Champ	Description
Nom	Spécifiez le nom que l'intégration utilise lorsqu'elle fait référence à cette UO. Le nom que vous entrez ici devient une cible LDAP dans l'enregistrement de source de données.
Nom distinct relatif à traiter	Spécifiez le nom distinct relatif du sous-répertoire que vous souhaitez rechercher. Ce NDR est combiné avec le répertoire de recherche de début de la définition du serveur LDAP pour identifier le sous-répertoire contenant des informations pour cette unité organisationnelle. Par exemple, l'exemple de définition d'unité organisationnelle utilise la valeur RDN `CN=Users` pour effectuer une recherche dans l'annuaire LDAP `CN=Users,DC=service-now,DC=com` et tout répertoire en dessous de ce point. Ce champ doit correspondre à un sous-répertoire dans votre système LDAP.
Champ d'interrogation	Spécifiez le nom de l'attribut dans le serveur LDAP pour interroger les enregistrements. Le champ de requête doit être unique dans les instances de domaine unique et multiple. Pour de meilleurs résultats, utilisez des adresses e-mail ou d'autres informations d'identification qui identifient de manière unique l'utilisateur dans une instance à domaines multiples. Active Directory utilise l'attribut **sAMAccountName** . D'autres serveurs LDAP ont tendance à utiliser l'attribut **cn** . **Remarque :** Le **champ Requête** doit être mappé au champ **ID d'utilisateur** dans la table Utilisateur [sys_user]. Par exemple, si un utilisateur Active Directory se connecte en tant que `joe.example`, il doit y avoir un enregistrement utilisateur avec une valeur **d'ID d'utilisateurjoe.example** et un enregistrement LDAP avec une valeur **sAMAccountNamejoe.example**.
Actif	Cochez cette case pour activer la définition d'OU et permettre aux administrateurs de tester l'importation des données. Toutefois, l'intégration ne peut apporter des données dans le système qu'à partir de définitions d'OU actives.
Table	Spécifiez la table qui reçoit les données mappées de votre serveur LDAP. Pour les utilisateurs, sélectionnez **Utilisateur (sys_user)** et pour les groupes, sélectionnez **Groupe (sys_group).**
Filtre	Saisissez une chaîne de filtre LDAP pour sélectionner les enregistrements spécifiques à importer à partir de l'UO. Plus la requête de filtre LDAP est spécifique, plus elle est efficace. Par exemple, la définition LDAP OU des utilisateurs utilise le filtre suivant pour sélectionner les enregistrements qui sont classifiés comme une personne, qui ont une valeur d'attribut **sn** , qui ne sont pas des ordinateurs et qui ne sont pas marqués comme inactifs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	(&(objectClass=person)(sn=*)(!(objectClass=ordinateur)) (! (userAccountControl :1.2.840.113556.1.4.803 :=2))) Vous pouvez trouver une description de la syntaxe du filtre LDAP en recherchant la RFC des filtres LDAP sur Internet.

Example: Exemples de définitions d'unités organisationnelles

Supposons que vous ayez un serveur LDAP avec la structure de répertoire suivante :

dc=mon-domaine,dc=com

- ou=Groupes
  - cn=Développement
  - cn=RH
  - cn = Ventes
- ou=Utilisateurs
  - ou=Développement
  - ou=RH
  - ou=Ventes

Supposons également que vous souhaitiez exclure le groupe RH et les utilisateurs RH de l'application. Procédez comme suit :

1. Créez un enregistrement de serveur LDAP avec le répertoire de recherche de départ dc=my-domain,dc=com.
2. Créez un enregistrement de définition d'unité organisationnelle pour ou=Groupes avec un filtre permettant d'exclure cn=HR.
3. Créez un enregistrement de définition d'unité organisationnelle pour ou=Utilisateurs avec un filtre permettant d'exclure ou=HR.

Si vous ne spécifiez pas d'attributs ou de filtres supplémentaires avec une définition d'UO, la requête LDAP renvoie la sous-arborescence complète du répertoire de départ et du NDR.

Dans ces exemples, une définition d'unité organisationnelle avec la valeur RDN ou=Groups et aucun filtre aurait renvoyé tous les groupes. De même, une définition d'unité organisationnelle avec la valeur RDN ou=Users et aucun filtre aurait renvoyé tous les utilisateurs et les unités organisationnelles enfants.

Créer une source de données pour LDAP

Chaque définition d'unité organisationnelle (UO) LDAP possède sa propre liste connexe de sources de données.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Remarque :
Le **serveur LDAP** et la **définition LDAP OU** doivent être actifs pour que l'action de chargement de test fonctionne correctement. Lorsque le chargement de test est activé pour la première fois, le système échantillonne jusqu'à 20 enregistrements pour déterminer la longueur des champs de jeu d'importation. Si les enregistrements échantillonnés ne contiennent pas de valeurs pour le champ **ID d'utilisateur** , le système définit la longueur du champ pour toutes les importations ultérieures sur la longueur par défaut de 40. L'importation tronque toutes les données importées qui dépassent la longueur du champ de la table de jeux d'importation. En outre, le champ **ID d'utilisateur** est tronqué à un maximum de 40 caractères. Sachez que les 20 enregistrements chargés ne peuvent pas être transformés et sont uniquement destinés à des fins de test. Si les enregistrements de test contiennent des valeurs pour le champ **ID d'utilisateur** , la longueur du champ est définie en fonction de la longueur du champ de l'ID d'utilisateur le plus long dans les enregistrements de test.

Pour créer une nouvelle source de données :

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Dans la liste connexe **Définitions d'unités organisationnelles LDAP** , sélectionnez un élément, tel que **Groupes** ou **Utilisateurs**.
4. Dans la liste connexe **Sources de données** , cliquez sur **Nouveau**.
5. Remplissez le formulaire Source de données (voir table).
6. Cliquez sur **Envoyer**.
7. Sous **Liens connexes**, cliquez sur **Tester le chargement de 20 enregistrements** pour tester si la source de données peut importer des données LDAP dans la table d'importation.

Formulaire Sources de données

Champ	Description
Nom	Spécifiez le nom que l'intégration utilise lorsqu'elle fait référence à cette source de données.
Nom de la table des ensembles de données à importer	Entrez le nom de la table intermédiaire où le système place temporairement les enregistrements et attributs LDAP importés. Examinez cette table pour afficher les enregistrements LDAP importés. Vous pouvez utiliser le même nom de table de jeu d'importation pour toutes les sources de données LDAP.
Type	Sélectionnez **LDAP** pour indiquer que les données importées sont des données LDAP. Une fois que vous avez sélectionné le type **LDAP**, le formulaire affiche le champ **cible LDAP** .
Cible LDAP	Sélectionnez la définition d'unité organisationnelle LDAP associée à cette source de données.

Mise en service automatique des utilisateurs LDAP

Vous mettez automatiquement en service les utilisateurs qui se trouvent dans le serveur LDAP, mais pas encore dans votre instance.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Créez les propriétés suivantes dans la table Propriétés système [sys_properties] :

Propriétés LDAP

Propriété LDAP	Description
glide.ldap.authentication	Active LDAP Authentication en utilisant LDAP pour authentifier les utilisateurs. Définissez cette propriété sur **vrai** (la valeur par défaut).
glide.ldap.user.autoprovision	Permet à LDAP le système de créer automatiquement des utilisateurs dans la table Utilisateur [sys_user] lorsque l'utilisateur existe dans LDAP, mais n'est pas encore dans l'instance. Définissez cette propriété sur **vrai** (la valeur par défaut).

Ces deux propriétés doivent être définies sur **vrai** pour que la mise en service automatique fonctionne.

Intégration LDAP via Serveur MID

Les administrateurs peuvent intégrer à l'aide d'une source de données LDAP sur un serveur MID (Management, Instrumentation, and Discovery).

Le serveur MID permet la communication et le mouvement de données entre les applications, les sources de données et les ServiceNow AI Platform services externes. Pour plus d'informations sur l'installation d'un Serveur MID, voir Installation du Serveur MID .

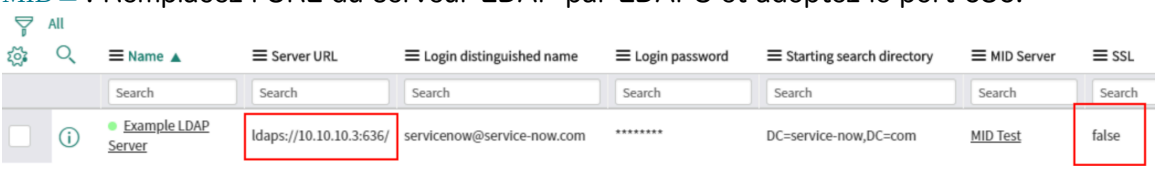
L'utilisation d'un serveur MID pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il élimine la nécessité d'établir un tunnel VPN entre votre serveur LDAP et vos centres de données. L'utilisateur du Serveur MID doit avoir le rôle user_admin pour pouvoir lire les enregistrements de configuration du serveur LDAP.

Remarque :
Le serveur MID n'autorise pas l'utilisation de l'action d'interface utilisateur `<instance>/sys_ui_action.do ?sys_id=1b4f7ef30a0001060058e223c9a5744c` pour actualiser les enregistrements d'utilisateur et de groupe à partir de LDAP.

Une connexion au Serveur MID communique via HTTP sur le port 80 par défaut. Ce canal de communication ne nécessite pas de certificat. La connexion entre le serveur MID et l'instance se fait via HTTPS (port 443). L'instance se connecte directement au serveur LDAP à l'aide de LDAP ou LDAPS. Cette connexion peut se faire soit par Internet, soit via un tunnel VPN.

Remarque :
LDAP ne peut pas communiquer via le serveur MID avec authentification par mot de passe.

Pour une communication sécurisée via SSL, vous devez ajouter un certificat SSL pour le serveur MID . Remplacez l'URL du serveur LDAP par LDAPS et adoptez le port 636.



Remarque :
Si vous créez un serveur LDAP, le marqueur SSL du serveur MID est défini sur false par défaut. Vous pouvez ignorer ce comportement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour définir les propriétés de connexion d'un serveur LDAP spécifique, reportez-vous à la section Définir un serveur LDAP.

Configurer la surveillance des connexions LDAP

Modifiez ou désactivez la surveillance des connexions LDAP et les notifications.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
L'instance envoie automatiquement un e-mail aux utilisateurs configurés dans le groupe d'administrateurs LDAP en cas d'échec d'une connexion au serveur LDAP. Cela utilise la notification par e-mail , qui est lancée par la tâche planifiée **Test de la connexion LDAP**. Cette notification par e-mail est activée par défaut.

Remarque :
L'instance n'envoie pas de notification par e-mail, sauf s'il y a au moins un membre dans le groupe d'administrateurs LDAP. Assurez-vous de renseigner ce groupe avec les utilisateurs que vous souhaitez recevoir l'e-mail.

Par défaut, la tâche planifiée teste la connexion toutes les 15 minutes. Pour modifier cet intervalle ou désactiver la surveillance :

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.
2. Ouvrez le **test de connexion LDAP**.
3. Effectuez l'une des actions suivantes :
   - Modifiez l'intervalle dans le champ **Intervalle de répétition** .
   - Désactivez la surveillance en décochant la case **Actif** .

Importer des données binaires via un serveur MID

En tant qu'administrateur, vous pouvez importer des données BLOB (Binary Large Object) avec une intégration LDAP via le MID Server.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Ajoutez le nom de la colonne LDAP à partir de laquelle vous souhaitez importer des données binaires dans la `glide.ldap.binary_attributes` de propriétés système.
2. Ajoutez une propriété du serveur MID avec le `nom glide.ldap.binary_attributes` et la même valeur que celle que vous avez définie pour la propriété système.

Dépannage de l'intégration LDAP via Serveur MID

Vous pouvez rencontrer des problèmes dans les domaines suivants lors de l'intégration de LDAP via Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez résoudre ces problèmes en consultant les sorties trouvées dans la file d'attente ECC (External Communication Channel) (**Découverte** > **Résultats et artefacts** > **File d'attente ECC**).

Problèmes de test de la connexion

Lors de la définition des unités organisationnelles au sein du serveur, une liste connexe Test de la **connexion** est utilisée pour vérifier la connexion LDAP. Lorsque vous cliquez sur ce lien, la file d'attente ECC doit afficher un message de sortie unique avec un nom de rubrique **LDAPConnectionTesterProbe**. Une fois le test terminé sur le serveur MID, la file d'attente ECC doit afficher un message d'entrée avec le même nom de rubrique. Si la colonne **Nom** du message d'entrée indique **vrai,** le test a réussi. Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'elle ne contient pas de messages d'erreur.

Test de la connexion

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Parcourir les problèmes

Lors de la définition des unités organisationnelles dans le serveur, il existe une liste connexe **Parcourir** qui est utilisée pour afficher les enregistrements de répertoire LDAP que la définition d'unité organisationnelle renvoie. Lorsque vous cliquez sur ce lien, la file d'attente ECC doit afficher un message de sortie unique avec un nom de rubrique **LDAPBrowseProbe**. Une fois les données renvoyées par le serveur MID, la file d'attente ECC doit afficher un message d'entrée portant le même nom. Si la colonne **Nom** du message d'entrée indique **vrai,** le test a réussi. Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'elle ne contient pas de messages d'erreur.

Problèmes de chargement d'importation

Lors du chargement de données (par exemple, à l'aide de la fonctionnalité Tester le chargement de 20 enregistrements), la file d'attente ECC doit afficher un message de sortie unique avec un nom de rubrique **LDAPProbe**.

Une fois les données renvoyées par le serveur MID, la file d'attente ECC doit afficher un autre message d'entrée appelé **LDAPProbeCompleted**. La colonne **Nom** de ce message d'entrée affiche le nombre total d'enregistrements renvoyés.

Un message d'entrée supplémentaire, également appelé **LDAPProbe**, s'affiche. La colonne **Nom** de ce message d'entrée affiche le numéro d'enregistrement le plus élevé du lot. Si le nombre total d'enregistrements renvoyés est de 258 et que la taille du lot est de 200 (la valeur par défaut), deux messages entrants LDAPProbe (200, 258) seront reçus, et un message entrant LDAPProbeCompleted (258) sera reçu.

Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'elle ne contient pas de messages d'erreur.

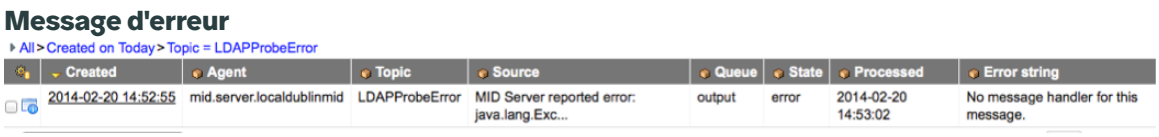
Chargement de l'importation

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Gardez également un œil sur un message de sortie appelé **LDAPProbeError**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur le lien dans la colonne **Nom** pour afficher les détails de l'erreur.

Pagination LDAP

La pagination LDAP ne fonctionne pas si la taille de pagination sur le serveur LDAP est inférieure à 1 000. Définir la propriété `glide.ldap.max_results` de Serveur MID sur une valeur inférieure ou égale à la taille de pagination du serveur LDAP.

LDAP échoue à importer des données binaires

Pour importer des données binaires via LDAP, telles qu'une photo d'utilisateur, vous devez inclure l'attribut binaire dans la propriété `glide.ldap.binary_attributes`Serveur MID . Pour l'exemple de la photo de l'utilisateur, l'attribut peut être jpegphoto.

Importer et mapper des données

Les mappages d'importation LDAP font correspondre les champs de votre base de données LDAP aux champs de votre instance.

Remarque :
Le mappage LDAP ayant un impact sur les performances, il est recommandé de le programmer en dehors des heures de pointe ou de traiter quelques enregistrements à la fois pour maintenir la disponibilité du système.

Définissez une carte de transformation qui importe uniquement les attributs nécessaires ou requis. Selon la version de l'instance que vous utilisez, la méthode de spécification des relations de mappage LDAP varie.

Pour savoir si vous exécutez ou non une version qui utilise l'application LDAP système pour l'intégration LDAP consiste à rechercher l'application à partir du navigateur d'application.

L'option **Exécuter les règles métier** n'est appliquée qu'à la table cible. Seules les cartes de transformation associées à la table cible exécutent les règles métier associées à différentes tables. Si vous mettez à jour un groupe d'utilisateurs et que des règles métier s'exécutent sur une table de groupe d'utilisateurs, le groupe doit avoir des rôles définis.

Options de mappage d'importation LDAP

Application système LDAP ?	Carte
Oui	Utilisez une *carte de transformation* pour spécifier votre mappage.
Non	Utilisez une *carte d'importation LDAP héritée* pour spécifier votre mappage ou la transformation LDAP par défaut incluse dans les instances de base de référence. N'oubliez pas d'ajuster le champ **Fusion** pour qu'il corresponde aux champs corrects.

Importations planifiées

Une importation planifiée permet aux administrateurs d'importer des données LDAP selon un calendrier régulier. Par défaut, l'intégration LDAP inclut deux exemples d'importations planifiées :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Exemple d'importation d'utilisateur LDAP
- Exemple d'importation de groupe LDAP

Aucun des exemples n'est actif par défaut. Modifiez ces importations planifiées pour répondre aux besoins professionnels de votre entreprise.

Cartes de transformation LDAP

La carte de transformation déplace les données de la table de jeux d'importation vers la table cible (Utilisateur ou Groupe).

L'intégration LDAP utilise des jeux d'importation et des cartes de transformation standard. Vous pouvez également créer des cartes de transformation LDAP personnalisées.

Important :
Que vous sélectionniez ou créiez des cartes de transformation LDAP personnalisées, une carte de transformation doit être active pour un ensemble de tables source et cible. L'activation de plusieurs cartes de transformation pour les mêmes tables source et cible peut produire des entrées en double dans la table cible, sauf si vous fusionnez avec les champs correspondants.

Cartes de transformation LDAP par défaut

Par défaut, le système fournit deux cartes de transformation pour les données LDAP.

Cartes de transformation LDAP par défaut

Carte de transformation	Table source	Table cible	Description
Importation d'utilisateur LDAP	[ldap_import]	[sys_user]	Carte de transformation par défaut pour la création d'enregistrements d'utilisateurs à partir des informations d'identification LDAP dans le cadre de la connexion LDAP à la demande. Contient des mappages pour un serveur LDAP Active Directory.
Importation de groupe LDAP	[ldap_group_import]	[sys_user_group]	Carte de transformation par défaut pour la création d'enregistrements de groupe à partir d'unités d'organisation LDAP. Contient des mappages pour un serveur LDAP Active Directory.

Remarque :
Par défaut, le système ne dispose pas d'une carte de transformation pour les enregistrements de département LDAP.

Conditions requises pour les cartes de transformation LDAP personnalisées

Si vous choisissez de créer une carte de transformation personnalisée, celle-ci doit répondre aux exigences de mappage suivantes.

Conditions requises pour les cartes de transformation LDAP personnalisées

Table source	Champ source	Table cible	Champ cible	Fusion	Description
ldap_import	u_source	sys_user	source	Faux	Le champ **u_source** identifie le ND LDAP de l'utilisateur ou

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions requises pour les cartes de transformation LDAP personnalisées (suite)

Table source	Champ source	Table cible	Champ cible	Fusion	Description
					du groupe importé. Le système utilise ce champ pour déterminer si un utilisateur a besoin d'une authentification LDAP, pour trouver le gestionnaire d'un utilisateur et pour placer les utilisateurs dans des groupes.
ldap_import	Sélectionnez l'un des champs suivants : • u_samaccountname • u_dn • u_cn	sys_user	user_name	vrai	Si LDAP **s'intègre** à Active Directory, sélectionnez u_samaccountname comme champ source. Si d'autres répertoires LDAP sont utilisés, sélectionnez **u_dn** ou **u_cn** comme champ source.

Différences entre les cartes de transformation LDAP et les cartes d'importation héritées

Lors de la spécification des relations de mappage LDAP à l'aide de cartes de transformation, il existe une différence majeure dans la façon dont les champs de référence sont définis pour le gestionnaire et le département.

Lors de l'utilisation d'une *carte de transformation*, il est nécessaire d'utiliser un *script de transformation* pour créer des références. Cela est dû au fait que la valeur associée à un attribut LDAP comme « gestionnaire » est le nom unique (DN) du gestionnaire.

Sans logique supplémentaire, le résultat est la création d'un enregistrement utilisateur avec un nom de gestionnaire qui est le nom unique de cet utilisateur dans LDAP. L'intégration inclut un script de transformation pour faciliter la création de ces références. La carte de transformation par défaut « Importation d'utilisateurs LDAP » inclut des scripts de transformation pour ces références.

Relations de mappage existantes

Lors de la mise à jour des cartes d'importation héritées vers des cartes de transformation, vous pouvez conserver les relations de mappage LDAP qui existaient avant l'ajout de l'application LDAP système. Le serveur LDAP possède un champ **Carte** qui fait référence à la carte d'importation héritée.

Remarque :
Par défaut, ce champ est masqué, vous devez donc configurer le formulaire pour l'afficher.

Si vous souhaitez passer à l'utilisation d'une carte de transformation, effacez la référence à la carte d'importation héritée.

Paramètres de mappage d'importation LDAP

Vérifiez et utilisez des attributs pour limiter les champs que l'intégration importe à partir de la source LDAP. En outre, il est important de mapper le champ user_name à l'attribut LDAP qui contient l'ID de connexion de l'utilisateur. Pour Active Directory, il s'agit généralement de l'attribut sAMAccountName. Si vous souhaitez importer et fusionner sur un attribut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

binaire (tel que objectSID ou objectGUID), vous devez créer un script de transformation personnalisé.

Remarque :
Toute valeur mappée au champ user_name doit être unique.

Si vous ne spécifiez pas de carte de transformation (telle que LDAP User Import), l'intégration utilise les mappages par défaut suivants :

Mappage par défaut de l'importation LDAP

Variable ou champ d'utilisateur	Attribut LDAP
user_name	sAMAccountName
E-mail	courrier
Téléphone	Numéro de téléphone
home_phone	Téléphone du domicile
mobile_phone	mobile
first_name	givenName
last_name	Sn
Titre	Titre
département	département
responsable	responsable
middle_name	paraphe
u_memberof	groupes
u_member	membres
u_manager	responsable

Transformation des données LDAP

Si un attribut LDAP contient des données simples, la carte de transformation lie un attribut LDAP importé à un champ approprié dans la table cible (Utilisateur ou Groupe). Par exemple, les exemples de données de l'attribut sAMAccountName sont mappées au champ **ID d'utilisateur** de la table Utilisateur.

Si les données LDAP importées sont mappées à un champ de référence, l'instance recherche un enregistrement correspondant existant. S'il n'existe aucun enregistrement correspondant, l'instance crée un nouvel enregistrement pour le champ de référence, sauf indication contraire du mappage de champs.

Par exemple, supposons que l'attribut LDAP l est mappé au champ de référence **Emplacement** de la table Utilisateur. Chaque fois que l'importation apporte une valeur d'attribut qui ne correspond pas à une valeur d'enregistrement d'emplacement existante, la carte de transformation crée un nouvel enregistrement d'emplacement. Le nouvel enregistrement d'emplacement a la même valeur que l'attribut importé et l'enregistrement d'utilisateur importé a maintenant un lien vers le nouvel enregistrement d'emplacement.

Toutefois, il arrive que l'attribut LDAP retourne un nom unique (DN), qui est essentiellement une référence à un autre enregistrement dans l'annuaire LDAP. Par exemple, l'attribut gestionnaire contient généralement le nom unique du gestionnaire de l'entrée de répertoire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

LDAP actuelle. Un DN importé utilise généralement une longue chaîne de texte telle que : cn=Beth Anglin,ou=Users,dc=my-domain,dc=com.

⚠ Avertissement :
Assurez-vous que vos champs cibles sont suffisamment longs pour contenir un DN. De nombreux champs de texte utilisent la longueur par défaut de 40, ce qui peut ne pas être suffisant pour certaines valeurs DN. Le ServiceNow système tronque toute valeur qui dépasse la longueur du champ.

En général, les administrateurs ne souhaitent pas que le système crée de nouveaux utilisateurs à partir de la valeur DN, car le nouvel utilisateur n'a aucune association avec un utilisateur existant. Au lieu de cela, les administrateurs souhaitent que l'importation localise l'enregistrement utilisateur existant du gestionnaire et l'associe à l'utilisateur nouvellement importé. L'include de script LDAPUtils contient les fonctions setManager et processManagers qui permettent d'analyser un DN et de rechercher un utilisateur existant. Pour de meilleurs résultats, utilisez ces fonctions pour créer une carte de transformation personnalisée.

Par exemple, le script de carte de transformation d'importation d'utilisateur LDAP appelle la fonction setManager :

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

Dans certains cas, l'intégration importe l'enregistrement d'un utilisateur avant l'enregistrement utilisateur du gestionnaire associé. Pour gérer de tels cas, vous pouvez appeler la fonction processManagers une fois la transformation terminée. Par exemple, la carte de transformation **d'importation d'utilisateur LDAP** utilise un script de transformation onComplete pour appeler la fonction processManagers .

```
// It is possible that the manager for a user did not exist in the database when // the
 user was processed and therefore we could not locate and set the manager field. // The
 processManagers call below will find all those records for which a manager could  // not be
 found and attempt to locate the manager again. This happens at the end of the  // import and
 therefore all users should have been created and we should be able to  // locate the manager
 at this point
ldapUtils. processManagers ( ) ;
```

Supprimez ou commentez les appels de fonction setManager et processManagers si votre intégration LDAP n'utilise pas l'attribut manager.

Écriture de scripts LDAP

Créez des cartes de transformation, des scripts et des règles métier personnalisés pour spécifier les exigences lors de l'importation de données.

Les cartes de transformation personnalisées doivent inclure les scripts de transformation onStart et onAfter .

Le script onStart doit appeler l'include de script LDAPUtils et commencer la connexion. Par exemple, la carte de transformation **d'importation d'utilisateurs LDAP** possède un script onStart qui utilise le code suivant :

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le script onAfter doit appeler la fonction addMembers . Par exemple :

```
ldapUtils.addMembers (source , target ) ;
```

Définir les utilisateurs Active Directory désactivés sur inactifs

Utilisez le script suivant pour désactiver automatiquement des utilisateurs lorsque l'utilisateur AD associé est désactivé.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les utilisateurs Active Directory désactivés en vérifiant la valeur de l'attribut userAccountControl . Cette règle s'exécute chaque fois que la valeur userAccountControl change et désactive les comptes utilisateur si le **contrôle de compte utilisateur** signifie un compte AD désactivé.

Utilisez le script suivant pour désactiver automatiquement des utilisateurs lorsque l'utilisateur AD associé est désactivé.

Procédure

1. Configurez le formulaire Utilisateur et créez un nouveau champ de nombre entier appelé **Contrôle de compte d'utilisateur**.
2. Ajoutez un mappage pour userAccountControl (externe) au nouveau champ.
3. Créez une règle métier avec les propriétés suivantes :

Désactiver la règle métier Utilisateurs AD

Champ de règle métier	Valeur
Nom	Désactiver les utilisateurs AD
Table	Utilisateur [sys_user]
Quand	Avant
Condition	current.u_user_account_control.changes()

Le champ Script doit contenir les éléments suivants :

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' +
 current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

Affecter des valeurs de champ LDAP

Vous pouvez utiliser un script pour affecter une valeur à n'importe quel champ pour lequel il existe un mappage de champ.

Par exemple, pour affecter une valeur au champ sys_user.société, créez une carte de champs pour le champ société et ajoutez un script de transformation des éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
company = "Don's Sporting Goods";
```

Exclure des utilisateurs LDAP particuliers

Si vous ne pouvez pas filtrer complètement la liste des utilisateurs LDAP à l'aide des propriétés de filtre LDAP, vous pouvez exclure les utilisateurs avec un script de carte.

Après avoir exécuté la logique pour identifier un utilisateur qui ne doit pas être importé, définissez le champ user_name sur une chaîne vide et cet utilisateur ne sera pas importé.

```
user_name='';
```

Une façon d'identifier les utilisateurs à filtrer consiste à rechercher une chaîne dans l'attribut distinguishedName . Par exemple, ce script exclut les comptes qui ne sont pas dans une unité organisationnelle d'utilisateur. Vous pouvez utiliser ce script si vous avez trop d'unités organisationnelles d'utilisateurs à inclure dans l'option LDAP d'unité organisationnelle cible.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

Une méthode de filtrage plus complexe consiste à utiliser des expressions régulières.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Définir l'action de choix pour les importations de champ de référence

La carte de transformation LDAP détermine la façon dont les champs de la table Jeu d'importation sont mappés aux champs de tables existantes telles que Incident ou Utilisateur.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Si la carte de transformation LDAP met à jour un champ dans la table de jeux d'importation, l'intégration crée automatiquement un nouvel enregistrement chaque fois qu'un nouvel enregistrement se trouve dans les données LDAP. Si la carte de transformation LDAP met à jour un champ de référence stockant des données d'une autre table, l'administrateur peut choisir de créer, d'ignorer ou de rejeter de nouveaux enregistrements LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, si l'intégration reçoit un nouvel enregistrement de département qui ne correspond à aucun département existant, vous pouvez mettre à jour tous les autres champs d'enregistrement LDAP sans créer de nouvel enregistrement de département dans l'instance. La carte de transformation vous permet de définir les options de création d'enregistrement pour chaque champ de référence.

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Cartes de transformation**.
2. Dans la liste connexe Cartes de champs, sélectionnez l'une des actions suivantes dans le champ **d'action Choix** :
   - **Créer** : crée un nouvel enregistrement de champ de référence si un enregistrement correspondant n'existe pas.
   - **Ignorer** : ignore les nouveaux enregistrements dans le champ de référence et termine le traitement de tous les autres champs dans la carte de transformation.
   - **Rejeter** : arrête la transformation pour l'enregistrement entier.

Remarque :
La carte de champs affiche uniquement le champ **d'action de choix** pour les champs de référence.

Vérifier le mappage LDAP

Après avoir créé une carte de transformation LDAP, actualisez les données LDAP pour vérifier que la carte de transformation fonctionne comme prévu.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Système LDAP** > **Charges planifiées**.
2. Cliquez sur votre tâche d'importation LDAP.
3. Cliquez sur **Exécuter maintenant**.

Dépannage de l'intégration LDAP

Si vous intégrez votre serveur LDAP et que vous avez des questions, ces éléments peuvent vous aider à résoudre le problème.

Vérifications préalables

- Si LDAP n'est pas disponible, les utilisateurs ne peuvent pas se connecter à l'instance. Une bonne pratique consiste à avoir des comptes locaux pour les administrateurs afin que les administrateurs puissent toujours accéder à l'instance si le LDAP est en panne.
- Vérifiez le compte de service pour vous assurer qu'il n'est pas expiré ou verrouillé.
- Vérifiez le format du nom d'utilisateur. Au lieu d'utiliser uniquement le nom d'utilisateur, essayez d'utiliser le domaine avec le nom d'utilisateur ou username@domain.
- Vérifiez que vous avez modifié l'entrée de `system_id` sur l'enregistrement `ldap_server_config` . Si vous modifiez le `system_id` involontairement avec un ensemble de mises à jour, `system_id` pointe vers le mauvais nœud pour l'instance cible et ne fonctionne pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Codes d'erreur

Le fichier journal LDAP répertorie les codes d'erreur standard du secteur pour LDAP et Active Directory (AD). Le fichier journal LDAP est contenu dans le fichier wrapper. Les codes d'erreur LDAP sont des nombres à deux chiffres, tandis que les codes d'erreur Active Directory sont des nombres à trois chiffres. Pour obtenir la liste des codes d'erreur les plus courants, consultez Codes d'erreur LDAP.

Intégration multi-domaines

Vous pouvez intégrer plusieurs domaines au sein d'une même forêt ou dans des domaines totalement non approuvés. Il est recommandé de créer un enregistrement de serveur LDAP distinct pour chaque domaine. Chaque enregistrement de serveur LDAP doit pointer vers un contrôleur de domaine pour ce domaine donné. Cela signifie que vous devrez autoriser les connexions à chacun des contrôleurs de domaine. Plusieurs forêts AD via LDAP avec un compte LDAP ne sont pas prises en charge.

Lorsque vous développez vers plusieurs domaines, il est essentiel d'identifier des attributs LDAP uniques pour les noms d'utilisateur de l'application et d'importer les valeurs de fusion. Un attribut de fusion unique commun pour Active Directory est `objectSid`. Les noms d'utilisateur uniques varient en fonction de la conception de vos données LDAP. Les attributs uniques courants sont `email` ou `userPrincipalName`.

Enregistrements entrants

Reportez-vous Cartes de transformation LDAP à la section pour définir comment l'intégration traite les enregistrements LDAP entrants pour lesquels il manque de valeurs correspondantes dans les champs de référence.

Erreurs d'authentification courantes

- L'utilisateur ne peut pas se connecter (DN non valide)
- CN non valide
- Connexion non valide

Tests de connexion LDAP automatiques

Vous pouvez tester manuellement les connexions aux serveurs LDAP ou autoriser ServiceNow le test automatique des connexions.

Le système teste automatiquement la connexion :

- Chaque fois qu'un utilisateur ouvre le formulaire du serveur LDAP.
- Via la tâche planifiée de test de connexion LDAP, qui s'exécute par défaut toutes les 15 minutes.

  Vous pouvez modifier la fréquence d'exécution de cette tâche planifiée. Si cette tâche planifiée n'est pas en mesure d'établir une connexion, une nouvelle tâche planifiée ponctuelle retente le test de connexion après cinq minutes ou après la moitié de la valeur **Intervalle de répétition** dans la tâche planifiée, selon la première éventualité.

Des messages d'erreur s'affichent sur le formulaire en cas de problème de connexion au serveur LDAP. Les connexions de test pour les serveurs situés derrière un serveur MID sont également prises en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher le moniteur LDAP

Vous pouvez afficher les informations actuelles sur les serveurs LDAP et les écouteurs à l'aide du moniteur LDAP.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les états disponibles sont les suivants :

- Actif
- Inactif
- Erreur
- Actif (arrêt...)
- Erreur (arrêt en cours...)

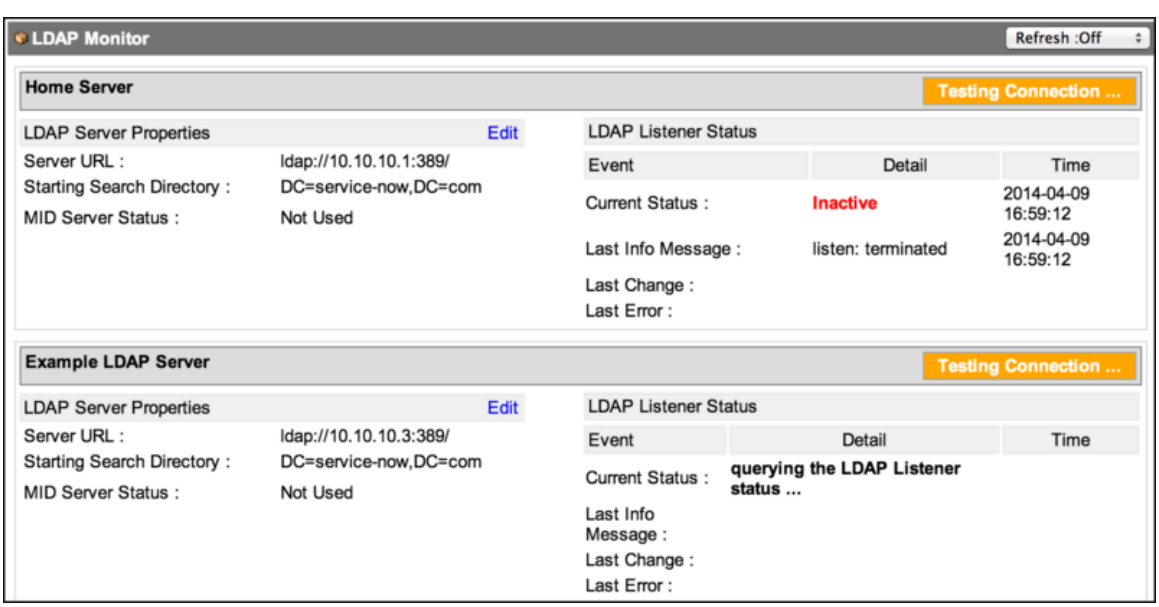
En plus de son état actuel, le moniteur affiche également :

- Dernier message détecté par l'écouteur, par exemple attente de changements LDAP, erreur de connexion, etc.
- Le dernier changement d'utilisateur LDAP, tel qu'un nouvel utilisateur, un utilisateur mis à jour, etc.
- La dernière erreur qui s'est produite.

Pour afficher le moniteur LDAP :

Procédure

Accédez à la **Tous** > **LDAP** > **Système LDAP** > **Surveillance LDAP**.



Consultez la table pour obtenir une description des propriétés et des champs à l'écran.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Surveillance LDAP

Champ	Description
Actualiser	Vous pouvez configurer le taux d'actualisation en cliquant sur le champ **Actualiser** de la barre d'en-tête Moniteur du serveur LDAP et en sélectionnant le nombre de secondes entre chaque actualisation des données. Vous pouvez également sélectionner **Aucun** pour supprimer l'actualisation.
État de connexion	L'indicateur de connexion au serveur est situé sur le côté droit, au-dessus des champs État de l'écouteur LDAP. Lorsque le serveur est connecté, la zone est verte et indique *Connecté*. Lorsque le serveur n'est pas connecté, la zone est rouge et indique *Non connecté*. Lorsque la connexion au serveur est testée, la zone est jaune et affiche *Test de la connexion*.
Propriétés du serveur LDAP	
Modifier	Lorsque vous surveillez des serveurs LDAP, vous pouvez apporter des modifications aux propriétés en cliquant sur **Modifier** dans l'écran Moniteur du serveur LDAP.
URL serveur	Combinaison du nom du serveur et du port du serveur dans lequel le serveur LDAP écoute. Fréquemment, le port est défini sur l'une des options suivantes : • 389 : port par défaut pour la connexion à LDAP en texte clair • 636 : port standard pour se connecter à LDAP via une connexion SSL Exemple de valeur : ldap://10.10.10.3:389/ Votre serveur LDAP peut avoir plusieurs adresses URL. Cela n'établit PAS plusieurs structures de répertoires à partir desquelles vous pouvez importer des données, ce qui se fait en créant une autre entrée de serveur LDAP, mais prévoit une redondance lorsque vous avez plusieurs serveurs LDAP pour éviter un point de défaillance unique. Les adresses URL LDAP sont séparées par un espace, et le système essaie automatiquement chaque adresse de serveur à tour de rôle jusqu'à ce qu'une connexion valide puisse être établie.
Répertoire de recherche de départ	Répertoire de départ ou NDR (Nom Distinct Relatif) dans lequel le système commence à rechercher des utilisateurs ou des groupes. Exemple de valeur : DC=service-now,DC=com Aucune donnée AU-DESSUS de ce point n'est disponible pour l'importation. L'instance a une visibilité sur le répertoire spécifié et les répertoires EN DESSOUS dans la hiérarchie LDAP.
État du serveur MID	État actuel de la connexion du serveur MID.
État de l'écouteur LDAP	
État actuel	Cela indique si l'écouteur est actif.
Dernier message d'informations	Cela affiche le dernier message reçu par le serveur LDAP concernant les changements d'utilisateur et de groupe, ainsi que l'heure de réception du message.
Dernier changement	Cette option indique le dernier changement apporté au serveur LDAP et l'heure à laquelle il a été effectué.
Dernière erreur	La dernière erreur qui s'est produite sur le serveur LDAP est ainsi que l'heure à laquelle elle s'est produite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Codes d'erreur LDAP

Le fichier journal LDAP répertorie les codes d'erreur standard de l'industrie pour LDAP et Active Directory (AD).

Codes d'erreur standard

Erreurs LDAP standard

Code d'erreur/ de données	Texte	Description
0	LDAP_SUCCESS	Indique que l'opération client demandée s'est terminée avec succès.
2	LDAP_PROTOCOL_ERROR	Indique que le serveur a reçu une demande non valide ou mal formée du client.
3	LDAP_TIMELIMIT_EXCEEDED	Indique que la limite de temps de l'opération spécifiée par le client ou le serveur a été dépassée. Lors des opérations de recherche, les résultats incomplets sont renvoyés.
4	LDAP_SIZELIMIT_EXCEEDED	Indique que lors d'une opération de recherche, la limite de taille spécifiée par le client ou le serveur a été dépassée. Les résultats incomplets sont renvoyés.
5	LDAP_COMPARE_FALSE	N'indique pas une condition d'erreur. Indique que les résultats d'une opération de comparaison sont faux.
6	LDAP_COMPARE_TRUE	N'indique pas une condition d'erreur. Indique que les résultats d'une opération de comparaison sont vrais.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Indique que le client a demandé une méthode d'authentification non prise en charge par le serveur LDAP au cours d'une opération de liaison.
8	LDAP_STRONG_AUTH_REQUIRED	Indique l'un des éléments suivants : Dans les demandes de liaison, le serveur LDAP accepte uniquement l'authentification forte. Dans une demande client, le client a demandé une opération telle que la suppression qui nécessite une authentification forte. Dans un avis de déconnexion non sollicité, le serveur LDAP découvre que la sécurité protégeant la communication entre le client et le serveur a échoué de manière inattendue ou a été compromise.
9		Réservé.
10	LDAP_REFERRAL	N'indique pas une condition d'erreur. Dans LDAPv3, indique que le serveur ne détient

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		pas l'entrée cible de la demande, mais que les serveurs dans le champ de référence le peuvent.
11	LDAP_ADMINLIMIT_EXCEEDED	Indique qu'une limite du serveur LDAP définie par une autorité administrative a été dépassée.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indique que le serveur LDAP n'a pas été en mesure de satisfaire une demande car une ou plusieurs extensions critiques n'étaient pas disponibles. Le serveur ne prend pas en charge le contrôle ou le contrôle n'est pas approprié pour le type d'opération.
13	LDAP_CONFIDENTIALITY_REQUIRED	Indique que la session n'est pas protégée par un protocole tel que TLS (Transport Layer Security), qui assure la confidentialité de la session.
14	LDAP_SASL_BIND_IN_PROGRESS	N'indique pas une condition d'erreur, mais indique que le serveur est prêt pour l'étape suivante du processus. Le client doit envoyer au serveur le même mécanisme SASL pour continuer le processus.
15		Pas utilisé(e).
16	LDAP_NO_SUCH_ATTRIBUTE	Indique que l'attribut spécifié dans l'opération de modification ou de comparaison n'existe pas dans l'entrée.
17	LDAP_UNDEFINED_TYPE	Indique que l'attribut spécifié dans l'opération de modification ou d'ajout n'existe pas dans le schéma du serveur LDAP.
18	LDAP_INAPPROPRIATE_MATCHING	Indique que la règle de correspondance spécifiée dans le filtre de recherche ne correspond pas à une règle définie pour la syntaxe de l'attribut.
19	LDAP_CONSTRAINT_VIOLATION	Indique que la valeur d'attribut spécifiée dans une opération de modification, d'ajout ou de modification DN enfreint les contraintes imposées à l'attribut. La contrainte peut être de taille ou de contenu (chaîne uniquement, pas de binaire).
20	LDAP_TYPE_OR_VALUE_EXISTS	Indique que la valeur d'attribut spécifiée dans une opération de modification ou d'ajout existe déjà en tant que valeur pour cet attribut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
21	LDAP_INVALID_SYNTAX	Indique que la valeur d'attribut spécifiée dans une opération d'ajout, de comparaison ou de modification est une syntaxe non reconnue ou non valide pour l'attribut.
22-31		Pas utilisé(e).
32	LDAP_NO_SUCH_OBJECT	Indique que l'objet cible est introuvable. Ce code n'est pas renvoyé pour les opérations suivantes : Recherchez des opérations qui trouvent la base de recherche, mais ne trouvent aucune entrée correspondant au filtre de recherche. Lier les opérations.
33	LDAP_ALIAS_PROBLEM	Indique qu'une erreur s'est produite lorsqu'un alias a été déréférencé.
34	LDAP_INVALID_DN_SYNTAX	Indique que la syntaxe du DN est incorrecte. (Si la syntaxe DN est correcte, mais que les règles de structure du serveur LDAP n'autorisent pas l'opération, le serveur renvoie le code 53 : LDAP_UNWILLING_TO_PERFORM.)
Ratio	LDAP_IS_LEAF	Indique que l'opération spécifiée ne peut pas être effectuée sur une entrée de feuille. (Ce code n'est actuellement pas dans les spécifications LDAP, mais est réservé pour cette constante.)
36	LDAP_ALIAS_DEREF_PROBLEM	Indique que lors d'une opération de recherche, le client n'a pas les droits d'accès pour lire le nom de l'objet aliasé ou que le déréférencement n'est pas autorisé.
37-47		Pas utilisé(e).
48	LDAP_INAPPROPRIATE_AUTH	Indique que, pendant une opération de liaison, le client tente d'utiliser une méthode d'authentification qu'il ne peut pas utiliser correctement. Par exemple, l'un ou l'autre des éléments suivants est à l'origine de cette erreur : Le client renvoie des informations d'identification simples lorsque des informations d'identification fortes sont requises... OU... Le client renvoie un ND et un mot de passe pour une liaison simple lorsque l'entrée n'a pas de mot de passe défini.
49	LDAP_INVALID_CREDENTIALS	Indique qu'au cours d'une opération de liaison, l'une des situations suivantes s'est produite : le client a transmis un ND ou un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		mot de passe incorrect, ou le mot de passe est incorrect car il a expiré, la détection d'un intrus a verrouillé le compte ou une autre raison similaire. Voir le code de données pour plus d'informations.
49 / 52e	AD_INVALID LES INFORMATIONS D'IDENTIFICATION	Indique une erreur Active Directory (AD) AcceptSecurityContext, qui est renvoyée lorsque le nom d'utilisateur est valide mais que la combinaison du mot de passe et des informations d'identification de l'utilisateur n'est pas valide. Il s'agit de l'équivalent AD du code d'erreur LDAP 49.
49 / 525	L'UTILISATEUR EST INTROUVABLE.	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est renvoyée lorsque le nom d'utilisateur n'est pas valide.
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indique une erreur de données Active Directory (AD) AcceptSecurityContext, c'est-à-dire que l'échec de la connexion est dû au fait que l'utilisateur n'est pas autorisé à se connecter pour l'instant. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification du mot de passe valides sont présentés.
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	Indique une erreur de données Active Directory (AD) AcceptSecurityContext, c'est-à-dire que l'échec de la connexion est dû au fait que l'utilisateur n'est pas autorisé à se connecter à partir de cet ordinateur. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification du mot de passe valides sont présentés.
49 / 532	PASSWORD_EXPIRED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec d'ouverture de session. Le mot de passe du compte spécifié a expiré. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides sont présentés.
49 / 533	ACCOUNT_DISABLED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec d'ouverture de session. Le compte est actuellement désactivé. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides sont présentés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	Indique que lors d'une tentative de connexion, le contexte de sécurité de l'utilisateur a accumulé trop d'ID de sécurité. Il s'agit d'un problème avec l'objet/le compte d'utilisateur LDAP spécifique qui devrait faire l'objet d'une enquête par l'administrateur LDAP.
49 / 701	ACCOUNT_EXPIRED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec d'ouverture de session. Le compte de l'utilisateur a expiré. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides sont présentés.
49 / 773	L'UTILISATEUR DOIT RÉINITIALISER LE MOT DE PASSE	Indique une erreur de données Active Directory (AD) AcceptSecurityContext. Le mot de passe de l'utilisateur doit être modifié avant de se connecter pour la première fois. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides sont présentés.
50	LDAP_INSUFFICIENT_ACCESS	Indique que l'appelant ne dispose pas des droits suffisants pour effectuer l'opération demandée.
51	LDAP_BUSY	Indique que le serveur LDAP est trop occupé pour traiter la demande client pour l'instant, mais que si le client attend et soumet à nouveau la demande, le serveur peut être en mesure de la traiter à ce moment-là.
52	LDAP_UNAVAILABLE	Indique que le serveur LDAP ne peut pas traiter la demande de liaison du client, généralement parce qu'il est en cours d'arrêt.
52e	AD_INVALID LES INFORMATIONS D'IDENTIFICATION	Indique une erreur Active Directory (AD) AcceptSecurityContext, qui est renvoyée lorsque le nom d'utilisateur est valide mais que la combinaison du mot de passe et des informations d'identification de l'utilisateur n'est pas valide. Il s'agit de l'équivalent AD du code d'erreur LDAP 49 : LDAP_INVALID_CREDENTIALS.
53	LDAP_UNWILLING_TO_PERFORM	Indique que le serveur LDAP ne peut pas traiter la demande en raison de restrictions définies par le serveur. Cette erreur est renvoyée pour les raisons suivantes : La demande d'ajout d'entrée enfreint les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		règles de structure du serveur... OU... La demande de modification d'attribut spécifie les attributs que les utilisateurs ne peuvent pas modifier. OU... Des restrictions de mot de passe empêchent l'action... OU... Des restrictions de connexion empêchent l'action.
54	LDAP_LOOP_DETECT	Indique que le client a découvert un alias ou une boucle de référence et qu'il n'est donc pas en mesure de terminer cette demande.
55-63		Pas utilisé(e).
64	LDAP_NAMING_VIOLATION	Indique que l'opération d'ajout ou de modification DN enfreint les règles de structure du schéma. Par exemple, La demande place l'entrée en position subordonnée à un alias. La demande place l'entrée subordonnée à un conteneur interdit par les règles d'imbrication. Le NDR de l'entrée utilise un type d'attribut interdit.
65	LDAP_OBJECT_CLASS_VIOLATION	Indique que l'opération ajouter, modifier ou modifier DN enfreint les règles de classe d'objet pour l'entrée. Par exemple, les types de demandes suivants renvoient cette erreur : L'opération d'ajout ou de modification tente d'ajouter une entrée sans valeur pour un attribut requis. L'opération d'ajout ou de modification tente d'ajouter une entrée avec une valeur pour un attribut que la définition de classe ne contient pas. L'opération de modification tente de supprimer un attribut requis sans supprimer la classe auxiliaire qui définit l'attribut comme requis.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Indique que l'opération demandée n'est autorisée que sur les entrées feuilles. Par exemple, les types de demandes suivants renvoient cette erreur : Le client demande une opération de suppression sur une entrée parente. Le client demande une opération de modification DN sur une entrée parente.
67	LDAP_NOT_ALLOWED_ON_RDN	Indique que l'opération de modification a tenté de supprimer une valeur d'attribut qui forme le nom distinct relatif de l'entrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
68	LDAP_ALREADY_EXISTS	Indique que l'opération d'ajout a tenté d'ajouter une entrée qui existe déjà, ou que l'opération de modification a tenté de renommer une entrée avec le nom d'une entrée qui existe déjà.
69	LDAP_NO_OBJECT_CLASS_MODS	Indique que l'opération de modification a tenté de modifier les règles de structure d'une classe d'objet.
70	LDAP_RESULTS_TOO_LARGE	Réservé pour CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Indique que l'opération de modification DN déplace l'entrée d'un serveur LDAP vers un autre et qu'elle requiert plusieurs serveurs LDAP.
72-79		Pas utilisé(e).
80	LDAP_OTHER	Indique une condition d'erreur inconnue. Il s'agit de la valeur par défaut pour les codes d'erreur NDS qui ne sont pas mappés à d'autres codes d'erreur LDAP.
775	USER_ACCOUNT_LOCKED	Indique que les utilisateurs ne peuvent pas se connecter car le compte d'utilisateur est verrouillé.

Codes d'erreur personnalisés

Codes d'erreur LDAP personnalisés

Code d'erreur/de données	Texte
10 000	LDAP_ERROR_GENEREL
10001	LDAP_ERROR_MAL_FORMED_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_ERROR_SOCKET_TIMEOUT
10302	LDAP_ERROR_CONNECTION_REFUSED
10303	LDAP_ERROR_CONNECTION_RESET
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Codes d'erreur LDAP personnalisés (suite)

Code d'erreur/de données	Texte
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_EXPIRED
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

Envoyer un mot de passe à usage unique lorsque le serveur LDAP est en panne

Une propriété LDAP permet d'envoyer un mot de passe à usage unique à un utilisateur si celui-ci n'est pas en mesure de se connecter parce que le serveur LDAP est en panne. Vous pouvez également configurer une autre propriété pour contrôler la durée de validité du mot de passe.

Avant de commencer

Rôle requis : admin

Pour recevoir un mot de passe à usage unique, les notifications doivent être activées sur le profil d'utilisateur de l'utilisateur. La notification est un e-mail uniquement. Les messages SMS ne sont pas pris en charge.

Pourquoi et quand exécuter cette tâche

Les deux propriétés sont activées par défaut. La valeur par défaut de la propriété qui contrôle la validité du mot de passe est de 10 minutes.

Procédure

1. Ouvrez la liste des propriétés système en saisissant `sys_properties.list` dans le filtre du navigateur d'application.
2. Trouvez la `glide.ldap.onetime.password.enabled` propriété.
3. Définissez la propriété sur `vrai`.
4. Pour modifier la durée de validité du mot de passe pour un utilisateur, définissez la propriété suivante sur un nombre entier de minutes : `glide.authenticate.onetime.password.validity`.

Synchronisation d'enregistrement LDAP

Les administrateurs peuvent synchroniser les enregistrements LDAP inactifs, désactivés ou supprimés avec leurs enregistrements LDAP.

La synchronisation des enregistrements LDAP est le processus de détection des enregistrements inactifs sur le serveur LDAP et de mise à jour des enregistrements LDAP correspondants. La détection des enregistrements LDAP inactifs implique la définition d'indicateurs de données cohérents pour chaque objet utilisateur, l'importation de données LDAP et l'évaluation des indicateurs de données.

Un indicateur de données peut être :

- Champ de date
- Appartenance à une UO spécifique (identifier en analysant l'attribut*dn*), à l'aide de l'attribut `useraccountcontrol`
- Une combinaison de ces indicateurs

Les données importées arrivent dans l'instance par le biais de tables de jeux d'importation où les données peuvent être évaluées et traitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le processus d'importation peut utiliser Actualiser les filtres LDAP sur plusieurs tâches d'importation pour diviser différents types d'enregistrements utilisateur et séparer les enregistrements pour un traitement séparé.

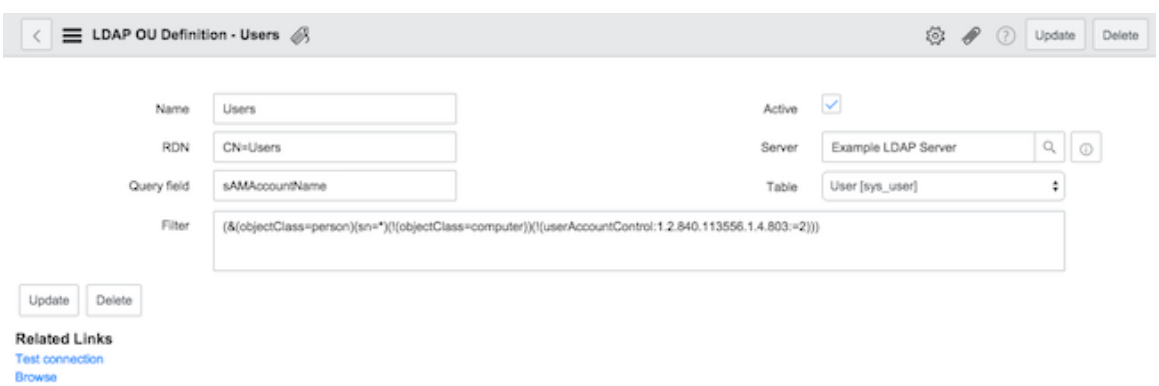
Actualiser les filtres LDAP

Les filtres du processus d'actualisation LDAP peuvent être utilisés pour spécifier un traitement qui ignore les insertions d'utilisateurs désactivés.

Vous pouvez desserrer le filtre LDAP OU pour importer toutes les données dans votre table de jeu d'importation (y compris les utilisateurs inactifs), puis spécifier un traitement qui ignore les insertions des utilisateurs désactivés. L'exemple de définition d'unité organisationnelle « Utilisateurs » fourni par l'instance dans son exemple LDAP prêt à l'emploi contient un filtre.

Ce filtre est important car il définit les enregistrements utilisateur à évaluer dans la table de jeux d'importation. Bien qu'il permette de réduire la charge de données, l'une des limites de ce filtre est qu'il filtre les utilisateurs inactifs, de sorte que les enregistrements d'utilisateurs inactifs ne sont pas importés dans les tables temporaires du jeu d'importation. Étant donné que les enregistrements d'utilisateurs inactifs ne sont pas visibles, il n'est pas possible d'évaluer les indicateurs d'enregistrement.

Filtre LDAP OU



Pour utiliser le filtrage dans le processus d'actualisation LDAP principal, modifiez le filtre pour afficher tous les enregistrements utilisateur. Par conséquent, tous les enregistrements seront chargés dans la table temporaire du jeu d'importation où ils pourront être évalués et transformés.

Remarque :
Il y a une précaution ici : comme le filtrage rassemble tous les enregistrements, vous risquez de vous retrouver avec un grand nombre d'anciens comptes LDAP inactifs qui ne doivent pas être insérés dans l'instance. Un enregistrement utilisateur ne doit jamais être créé pour un utilisateur handicapé.

Extraction LDAP

Un processus d'extraction LDAP peut être mis en œuvre pour détecter les utilisateurs désactivés.

Un extrait de votre source LDAP peut être filtré pour les utilisateurs désactivés à l'aide d'un marqueur actif qui peut être défini pour chaque enregistrement de l'importation sur « faux ». Spécifiez ('target.active=false') et copiez dans le champ **Script** directement sur l'enregistrement de la carte de transformation de table.

Avantages

Les avantages de cette méthode comprennent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Écriture de scripts simples
- Les enregistrements utilisateur existants ne sont pas impliqués dans le traitement
- Les utilisateurs inactifs ne sont pas chargés dans une table d'importation temporaire
- Aucun impact sur les performances

Inconvénients

Les inconvénients de cette méthode comprennent :

- Un processus supplémentaire est créé
- L'ensemble d'extraits doit être placé dans un emplacement où votre source de données peut y accéder

Méthode alternative

Actualiser les filtres LDAP Utilisez plusieurs tâches d'importation pour diviser différents types d'enregistrements utilisateur, en séparant les enregistrements pour un traitement séparé.

Comptes d'utilisateurs LDAP inactifs

Détecte qu'un compte utilisateur existant et actuel est inactif ou a été désactivé ou supprimé d'un LDAP Active Directory (AD).

Un problème courant de l'intégration LDAP est la façon de détecter les utilisateurs désactivés ou supprimés dans un Active Directory (AD), puis de les désactiver dans l'instance. Dans un LDAP Active Directory, un filtre est généralement défini pour exclure les utilisateurs inactifs lors de l'actualisation, de sorte que l'instance ne soit pas au courant des utilisateurs désactivés ou supprimés dans AD. La question est de savoir comment détecter qu'un utilisateur actuel existant est inactif ou a été supprimé d'AD.

Pour plus d'informations sur la localisation des comptes inactifs, consultez Rechercher des comptes LDAP inactifs à l'aide du champ userAccountControl .

Remarque :
L'approche recommandée consiste à *désactiver* les enregistrements utilisateur et tous les autres types d'enregistrements, et non à les supprimer. Chaque enregistrement est lié à d'autres enregistrements, et la suppression d'un enregistrement détruit toutes les relations avec ces autres enregistrements. La désactivation des enregistrements maintient ces relations en place.

Rechercher des comptes LDAP inactifs à l'aide du champ userAccountControl

Identifiez quand un utilisateur Active Directory (AD) est supprimé (ou rendu inactif).

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Une méthode consiste à suivre l'état actif des utilisateurs AD et à créer une règle métier pour mettre à jour les comptes correspondants lorsqu'un compte AD est inactif.

Procédure

1. Créez un champ de chaîne sur la table Utilisateur [sys_user] pour suivre la valeur du champ AD **userAccountControl** .
   Par exemple : `u_ad_user_account`.
2. Créez un script de transformation LDAP pour définir la valeur du champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example

```
target.u_ad_user_account = source.userAccountControl
```

3. Mettez à jour le filtre LDAP pour afficher les comptes AD désactivés.

   Example
   Voici un exemple de filtre.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Voici un exemple de filtre de remplacement que vous pouvez utiliser.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Créez une règle métier onChange pour définir le champ actif sur false chaque fois que le champ u_ad_user_account a la valeur 514.
   « 514 » indique un compte inactif.

Exemples de scripts LDAP

Les exemples de script suivants supposent que vous utilisez un Active Directory (AD) pour votre serveur LDAP.

Script des valeurs d'attributs userAccountControl

Cet exemple teste la source des valeurs d'attribut userAccountControl associées à un utilisateur désactivé (514 ou 546).

```
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
  target.active=false;
  target.locked_out=true;
}
```

Voici un exemple utilisant une vérification au niveau du bit :

```
if(source.u_useraccountcontrol & 2){
  active = false;
}
```

Script d'attribut userAccountControl

Cet exemple examine l'attribut userAccountControl mais ne teste pas de valeurs spécifiques. Il offre également la possibilité de réactiver les comptes d'utilisateurs LDAP.

```
/*
* Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
*/
if(ctrl.substr(-1) == "2"){

  //Deactivate and lock the user account
  target.active = false;
  target.locked_out = true;

  //Ignore any insert of a disabled record
  if(action == 'insert'){
    ignore = true;
  }
}
/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

Script de carte de transformation onBefore

Voici un exemple de script de carte de transformation onBefore. Le script identifie les enregistrements désactivés et les enregistrements en cours d'insertion. Si une insertion d'un utilisateur désactivé se produit, l'opération de transformation ignore l'enregistrement.

```
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
  ignore = true;
}
```

Script de membre DN

Cet exemple de script introduit une flexibilité en ne s'appuyant pas sur les valeurs 546 et 514 de userAccountControl, mais en vérifiant si l'utilisateur est membre d'un nom unique (DN) particulier. Vous pouvez utiliser ce script dans le champ **Script** de l'enregistrement « Carte de transformation de table » ou dans un script de carte de transformation onBefore.

```
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
  target.active = false;
  target.locked_out = true;
}
```

ADAM (Active Directory Application Mode)

ADAM (Active Directory Application Mode) est un service d'annuaire compatible LDAP (Lightweight Directory Access Protocol).

Remarque :
Un niveau de compréhension de base de Microsoft Windows Server et d'Active Directory est nécessaire pour comprendre cette rubrique. Vous devez également disposer des autorisations d'administrateur sur le serveur que vous configurez pour ADAM.

Ce sont des exemples de procédures. En raison des variations d'installation et d'environnement, nous ne pouvons pas offrir d'assistance directe. Nous vous recommandons de travailler avec un Microsoft consultant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ADAM a une installation simple et fonctionne en tant que service sur Windows les systèmes d'exploitation. Il peut être entièrement personnalisé et distribué en tant que composant d'application ou utilisé en tant que répertoire LDAP autonome. ADAM utilise les mêmes technologies que celles des contrôleurs de domaine Active Directory (y compris les fonctionnalités de réplication et de délégation) et possède ses propres fonctionnalités d'administration et de personnalisation. Il peut être exécuté en tant que Windows service. ADAM peut être installé sur Windows les systèmes d'exploitation XP, 2000, 2003 et 2008. ADAM est inclus dans Windows Server 2003 R2 et Windows Server 2008. Un téléchargement est disponible sur http://www.microsoft.com/downloads http://www.microsoft.com/downloads pour les systèmes d'exploitation antérieurs.

Sécurité

Certaines politiques de sécurité d'entreprise interdisent aux fournisseurs et partenaires externes de se connecter directement à un contrôleur de domaine Active Directory (AD). Si l'exposition de certains objets ou attributs AD à un fournisseur ou à un partenaire externe est interdite, l'accès aux objets et attributs peut être bloqué à l'aide des entrées de contrôle d'accès de sécurité AD (ACE OU ACL). Selon les exigences de sécurité, cette méthode peut introduire de la complexité dans l'intégration. Il est recommandé de consolider plusieurs domaines et forêts. Si toutes les importations et authentifications LDAP doivent être acheminées via une source unique, ADAM peut être utilisé comme source consolidée. Avec la sortie de Windows 2008, cette fonctionnalité a été renommée en Light-Weight-Directory Service, LDS. L'installation et la configuration sont similaires à celles de Windows Server 2003 R2.

Connaissances recommandées

Pour cette tâche, vous devez comprendre AD, les classes d'objets et les attributs. Pour une intégration réussie, vous devez connaître la structure d'objets AD actuelle, vous familiariser avec les délégations Active Directory et avoir une stratégie sur la façon d'utiliser ADAM et à quelles fins. Si vous n'êtes pas familier avec AD ou ADAM, travaillez avec votre administrateur AD pour configurer un nouvel environnement ADAM.

Fiducies

Si `des objets userProxy` sont utilisés, l'ordinateur hébergeant ADAM doit être membre du domaine qui possède les comptes AD ou membre d'un domaine de confiance.

Connectivité interne

Si `des objets userProxy` sont utilisés, l'ordinateur ADAM doit pouvoir se connecter aux contrôleurs de domaine connexes pour effectuer une authentification de proxy.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configuration d'une instance avec ADAM

La première installation copie les fichiers ADAM sur votre ordinateur, enregistre les composants requis et crée les raccourcis de l'application.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Par défaut, tous les fichiers d'application sont installés dans %systemroot %\ADAM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Windows Serveur 2003 R2 - ADAM peut être installé à l'aide du **Panneau de configuration > Ajouter et supprimer des programmes > Gestionnaire de composants facultatif**.
- Windows Server 2000 & Windows XP - Téléchargé http://www.microsoft.com/downloads sur Microsoft.

Créez le service de première instance qui fonctionne en tant que premier service d'annuaire hébergé par ADAM. Effectuez l'une des actions suivantes :

Procédure

- Exécutez `adaminstall.exe` à partir du dossier ADAM.
- Utilisez le raccourci **Créer une instance ADAM** à partir de **Menu Démarrer > programmes > ADAM** dossier.

1. Sélectionnez l'option **d'installation d'une instance unique** .

   Remarque :
   Vous pouvez utiliser cette option pour installer un réplica d'instance sur un deuxième serveur afin de fournir un système tolérant aux pannes.

2. Renseignez les champs.

ADAM Instance

Champ	Description
Nom d'instance	utilisé principalement pour identifier le nom et le nom d'affichage du Windows service
Ports	définit les numéros de port à utiliser pour les écouteurs LDAP et LDAPS. Le port LDAP par défaut est 389, LDAPS est 636. Si ces ports sont utilisés sur le serveur, l'assistant de configuration sélectionne de nouveaux ports. Collaborez avec votre administrateur réseau pour déterminer les meilleurs ports à utiliser
Partition du répertoire d'application	Crée une partition de répertoire d'application. N'étant pas nécessaire à cette étape, nous vous recommandons de créer la nouvelle partition maintenant. Une bonne pratique consiste à utiliser le même nom unique que votre forêt ou domaine, mais à remplacer le domaine de niveau le plus élevé par adam au lieu de com ou local. Par exemple, si votre partition de forêt est `dc=myCompany,dc=com`, vous pouvez créer la partition ADAM en tant que `dc=myCompany,dc=adam`
Emplacements de fichiers	sélectionne le ou les emplacements pour les données de partition ADAM.
Sélection du compte de service	Sélectionne un compte de service sous lequel l'instance s'exécute. Pour les services autonomes, vous pouvez utiliser le compte de service réseau par défaut. Si vous prévoyez d'utiliser des répliques, vous devez utiliser un compte qui a accès à toutes les instances ADAM.
Administrateurs ADAM	la délégation sur le répertoire ADAM qui exploite l'authentification intégrée Windows. Il s'agit de la manière dont l'accès initial est accordé pour l'administration. Une fois les droits accordés au compte initial, cet utilisateur ou ce groupe délègue des droits à d'autres utilisateurs Windows ou ADAM. Vous pouvez sélectionner la valeur par défaut pour accorder uniquement l'accès administrateur à l'utilisateur actuel ou accorder l'accès à un autre utilisateur ou groupe en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Importer des fichiers LDIF	les fichiers à importer. MS-UserProxy est le fichier le plus important à importer, mais cela vaut la peine d'ajouter tous les fichiers disponibles car il y a peu de surcharge au schéma et vous n'aurez pas à vous soucier de l'étendre plus tard si vos besoins augmentent. Confirmez les détails et l'assistant termine la configuration.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configurer la console ADAM

Configurez la console ADAM. Même s'il existe de nombreuses similitudes entre ADAM et Active Directory, l'administration peut être très différente puisqu'il n'y a pas de console **de gestion Utilisateurs et Ordinateurs** .

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La plupart de l'administration générale est effectuée à l'aide de la console ADAM ADSI MMC disponible dans le menu de démarrage **d'ADAM** . La première fois que vous exécutez la console ADAM ADSI, vous devez vous connecter à la partition que vous avez créée.

Procédure

1. Cliquez avec le bouton droit de la souris sur l'élément **de modification ADSI ADAM** dans le cadre de gauche.
2. Donnez un nom à la nouvelle connexion et mettez à jour les champs nom du serveur et port avec les informations utilisées lors de la création de l'instance.
3. Sélectionnez un **nom unique** ou un **contexte de dénomination** et spécifiez le nom unique de la partition d'application que vous avez créée précédemment.
   Vous pouvez vous connecter aux partitions `Configuration et Schéma` pour obtenir des options de configuration avancées.
   Vous devriez maintenant être en mesure de voir la partition et les conteneurs par défaut pour LostAndFound, NTDS Quotas et Roles. Le conteneur Rôles n'a pas encore été configuré.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Créer des conteneurs et des unités organisationnelles pour ADAM

Regroupez logiquement les objets stockés dans ADAM dans des conteneurs et des unités d'organisation (UO) comme ils le feraient dans Active Directory.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Cliquez avec le bouton droit sur la partition racine et accédez à **Nouveau** > **Objet** > **Unité organisationnelle**.

   Remarque :
   Vous pouvez également consulter la liste des autres objets disponibles. Cette liste varie en fonction des extensions de schéma installées lors de l'importation des fichiers LDF.

2. Lorsque vous êtes invité à saisir une valeur, saisissez le nom de l'UO telle que `Utilisateurs`.
   L'écran affiche un bouton **Plus d'attributs** .
3. Utilisez le bouton pour affecter des valeurs à des attributs supplémentaires.
   Pour les unités organisationnelles et les conteneurs, aucune valeur supplémentaire n'est nécessaire.
   Après avoir créé les unités d'organisation, les nouvelles unités d'organisation sont répertoriées comme enfants de l'objet racine.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Délégation avec ADAM

Une fois la structure de l'unité organisationnelle créée, définissez les délégations d'autorisation pour sécuriser correctement les objets pour les utilisateurs limités.

Comme pour Active Directory, il existe deux façons générales d'accorder des autorisations :

- Ajoutez des utilisateurs à un groupe auquel les autorisations appropriées sont déjà affectées.
- Définissez de nouvelles autorisations sur les objets ADAM.

Pour cette tâche, nous abordons les autorisations au niveau de l'objet. Reportez-vous à la section Administration des groupes pour plus d'informations sur les appartenances aux groupes.

Comme nous n'avons pas de console Utilisateurs et ordinateurs pour ADAM, toutes les autorisations au niveau de l'objet sont définies à l'aide de *`l'utilitaire`* Active Directory DSACLS.exe. Ce fichier se trouve dans le répertoire du programme ADAM. Lors de l'exécution des utilitaires ADAM, il est préférable de lancer l'invite de commande des outils ADAM. Cela garantit les versions appropriées des outils. DSALCS est utilisé pour afficher et définir les droits d'accès aux objets.

Exemple : « `dsacls \\localhost :50010\dc=myCompany,dc=adam` » affiche les autorisations affectées à la racine de la partition *`dc=myCompany,dc=adam`* en cours d'exécution sur le localhost, port 50010. DSACLS est un outil complexe utilisé pour créer une délégation complexe. Exécutez *`« DSACLS / ? »`* pour obtenir des notes d'utilisation.

Information associée

Créer des conteneurs et des unités organisationnelles pour ADAM

Utiliser ADAMSync pour renseigner ADAM

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Remplissage des objets ADAM

Les objets ADAM comprennent les objets utilisateur, l'objet UserProxy et les objets Group.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Objets utilisateur

Les utilisateurs peuvent être créés à l'aide de la console ADAM ADSI Edit comme nous l'avons fait pour la création d'OU. Les utilisateurs peuvent également être administrés à l'aide des outils de ligne de commande AD, ce qui n'entre pas dans le cadre de ce document. Le seul attribut obligatoire pour les nouveaux objets d'utilisateur est le *cn*, qui est un nom court ou le nom complet de l'utilisateur. Il existe également un large éventail d'attributs facultatifs similaires aux attributs d'utilisateur Active Directory. Vous pouvez accéder à la liste complète des attributs en sélectionnant les propriétés à partir de l'objet utilisateur.

Objets UserProxy

Pour ServiceNow l'intégration LDAP, nous vous recommandons d'utiliser des objets *UserProxy* dans ADAM qui crée un compte proxy lié au compte utilisateur AD associé. Cela vous permet de demander à ADAM d'authentifier les identifiants de connexion à l'aide des noms d'utilisateur et mots de passe AD du domaine sans ServiceNow se connecter directement au contrôleur de domaine. *Les objets UserProxy* sont très similaires aux objets AD et ADAM User, sauf qu'ils ne stockent pas de mots de passe et qu'ils ont un attribut *objectSID* qui contient le SID de l'objet AD User lié. Voici comment fonctionne le proxy. *Les objets UserProxy* sont créés à l'aide de la console *ADSIEdit* ou des outils de ligne de commande, mais cela peut être fastidieux. Il est recommandé d'utiliser un processus automatisé tel que défini ci-dessous.

Objets de groupe

Les groupes sont créés à l'aide de la console ADSIEdit et des outils de ligne de commande AD. Les concepts de groupe sont similaires à AD et sont utilisés pour intégrer des groupes et des membres à ServiceNow. La plus grande différence est que les groupes ADAM peuvent contenir des membres d'ADAM ou de domaines AD de confiance.

Automatisation de la création d'objets ADAM

Si vous souhaitez synchroniser des comptes Active Directory avec ADAM, nous vous recommandons d'utiliser Microsoft *ADAMSync* outil. Il s'agit de l'utilisation la plus courante d'ADAM pour ServiceNow l'intégration LDAP.

À propos de la délégation d'autorisation

ADAM contient des groupes intégrés avec des autorisations par défaut. Ces groupes se trouvent dans le conteneur *cn=roles,dc=myCompany,dc=adam*. Ceux-ci sont similaires aux groupes de niveau de domaine et ont des droits sur les objets de la partition actuelle. Comme pour les forêts AD, vous pouvez également définir un niveau d'autorisations plus élevé à l'aide des groupes par défaut dans *cn=roles,cn=configuration,dc=myCompany,dc=adam*. Vous devez vous connecter à la partition de configuration dans *ADSIEdit*. Le groupe Administrateurs inclut par défaut le compte spécifié lors de la configuration. Ce membre n'est pas toujours visible, car il est hérité via les groupes de configuration. Les administrateurs ont le contrôle total de tous les objets de partition. Le groupe Lecteurs ne contient aucun membre par défaut et dispose d'un accès en lecture à tous les objets de la partition. Le groupe Utilisateurs est un groupe dynamique, tout comme dans Active Directory. Transitivement, il inclut tous les utilisateurs ADAM créés dans la partition.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Test et dépannage de la configuration ADAM

Le principal outil utilisé pour le test est LDP. Cela vous permet de tester entièrement l'authentification de l'utilisateur.

La plupart de la gestion des objets peut être effectuée à l'aide de la console ADAM ADSI Edit qui permet d'accéder à l'ensemble de la collection d'objets et d'attributs. Le niveau le plus élevé de contrôle et de dépannage des services ADAM consiste à utiliser le Windows service créé lors de la configuration de l'instance. Le nom du service varie et dépend du nom de l'instance créée. Ce service doit être en cours d'exécution pour que le service ADAM s'exécute. Si vous rencontrez des problèmes de connexion, vous devez examiner les configurations réseau pour vous assurer que vous disposez de l'accès réseau approprié pour vous connecter au serveur et au port ADAM. Pour chaque instance ADAM installée, un journal des événements Windows est créé. C'est également un excellent outil pour dépanner les services ADAM.

Le Windows journal des événements de sécurité est également utile pour le dépannage des authentifications `userProxy` . Toutes les tentatives `d'ouverture de session userProxy` sont enregistrées dans le journal de sécurité et font référence à l'adresse de l'appareil client distant, au nom unique de l'utilisateur qui tente de se connecter et au code de résultat ou d'état.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Sauvegarde et restauration avec ADAM

Toutes les données ADAM peuvent être sauvegardées à l'aide de méthodes de sauvegarde de systèmes de fichiers standard.

Redondance

ADAM dispose d'utilitaires de réplication intégrés basés sur la même technologie qu'AD. Un réplica complet en lecture et écriture d'une partition ADAM peut exister sur le même ordinateur ou sur un ordinateur différent. Vous pouvez utiliser ce réplica de différentes manières pour fournir une intégration LDAP tolérante aux pannes avec l'instance. Une option consiste à exposer les deux partitions à l'instance via le pare-feu et à définir les deux serveurs dans le champ Serveur des propriétés LDAP.

Information associée

ADAM (Active Directory Application Mode)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Utiliser LDAPS avec ADAM

La configuration par défaut de l'authentification par objet `userProxy` consiste à appliquer les communications LDAPS (LDAP sécurisées). LDAPS nécessite des certificats SSL pour sécuriser le trafic réseau.

Pour supprimer cette exigence, apportez la modification suivante à l'aide de la console `ADSIEdit` connectée à la partition de configuration.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Redémarrez le service ADAM pour utiliser le nouveau paramètre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour prendre en charge les liaisons sécurisées et chiffrer les informations d'utilisateur et de mot de passe transmises, un certificat SSL doit être installé sur le serveur et tout client LDAP. Étant donné que les utilisations du service ADAM sont limitées et contrôlées, il est possible d'utiliser un certificat auto-signé qui répondrait aux besoins sans encourir de coûts de certificat ni construire une infrastructure d'autorité de certification (CA). Si vous avez déjà une autorité de certification, vous pouvez émettre un certificat. Sinon, créez un certificat auto-signé.

Création d'un certificat autosigné

Pour utiliser l'utilitaire `selfssl` , Internet Information Services (IIS) doit être installé. Ce service peut être supprimé après avoir généré le certificat. Vous pouvez obtenir l'utilitaire selfssl.exe à partir du kit de ressources IIS. Si IIS est déjà installé, créez un site web afin que les sites actuels ne soient pas impactés lors de la génération du certificat. Selfssl doit temporairement joindre le nouveau certificat auto-émis à un site Web valide.

Selfssl est un outil en ligne de commande et possède les paramètres communs suivants.

Descriptions des paramètres Selfssl

Paramètre	Description
/t	Ajoute le certificat aux « Certificats approuvés » sur l'ordinateur local
/N :cn	Définissez le nom commun du certificat. Celui-ci doit correspondre au nom de domaine complet du serveur exécutant le service Web à l'aide du certificat
/K	Définit la force de la taille de la clé en bits
/V	Nombre de jours de validité du certificat
/S	ID du site Web auquel joindre le certificat
/P	Port IP du service Web

L'attribut de nom commun doit correspondre au nom ou à l'adresse externe que l'instance utilisera pour se connecter à votre ordinateur ADAM. Vous devrez obtenir l'ID du site Web IIS, sauf si vous utilisez le site Web par défaut qui est 1 et n'a pas besoin d'être défini dans la commande selfssl. Voici un exemple de commande pour générer un certificat pour myCompany :

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

Cette instruction crée un certificat valable 10 ans. Définissez la valeur sur n'importe quelle durée, mais sachez que le nouveau certificat doit être généré et soumis à l'instance avant l'expiration de l'ancien. Nous vous recommandons de noter la date d'expiration sur le certificat.

Une fois le certificat généré, vous pouvez le supprimer du site Web ou supprimer l'ensemble du site Web si vous avez créé un site temporaire.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Affecter le certificat à ADAM

Installez un certificat SSL sur le serveur et tout client LDAP pour prendre en charge les liaisons sécurisées et chiffrer les informations d'utilisateur et de mot de passe transmises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Étant donné que les utilisations du service ADAM sont limitées et contrôlées, il est possible d'utiliser un certificat auto-signé pour répondre à vos besoins sans encourir de coûts de certificat ni construire une infrastructure d'autorité de certification (CA).

Procédure

1. Ouvrez la console MMC Certificats et créez deux connexions de console, l'une pour les certificats d'ordinateur local et l'autre pour les certificats de services informatiques locaux sur le nouveau service ADAM.
   Le nouveau certificat se trouve sous Certificats (ordinateur local)\Personnel\Certificats.
2. Copiez le certificat dans le conteneur pour les certificats de service ADAM – Service (nom de service ADAM)\ADAM_ADAM Nom de service\Certificats racines de confiance\Certificats et copiez le certificat dans Certificats – Service (Nom de service ADAM)\ADAM_ADAM Nom de service \Personnel\Certificats.
3. Ouvrez l'onglet Détails du certificat que vous avez copié, notez l'horodatage de début de validité et attribuez un accès en lecture au fichier de clé de certificat.
   Accédez à C :\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA \MachineKeys et identifiez le certificat avec l'horodatage correspondant. Attribuez des droits de lecture et d'exécution au compte de service exécutant ADAM. Par défaut, il s'agit **du service réseau**.
4. Redémarrez le service ADAM pour activer le nouveau certificat.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Exporter le certificat de clé publique

Les clients LDAPS, y compris l'instance, ont besoin du certificat de clé publique pour établir une connexion sécurisée à ADAM.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
À partir des consoles de certificat de serveur que vous avez utilisées ci-dessus, exportez une clé publique à utiliser par les clients.

Procédure

1. Sélectionnez le certificat, cliquez avec le bouton droit de la souris, puis sélectionnez **toutes les tâches/ exportations**.
   N'exportez pas la clé privée. Sélectionnez le format binaire codé DER X.509 par défaut et spécifiez le nom du fichier d'exportation.
2. Installez le certificat public sur les clients LDAP qui se connectent au serveur à l'aide de LDAPS.
   Lorsque vous y êtes invité, ajoutez le certificat au magasin des *`autorités de certification racines approuvées`*.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Compte d'accès en mode d'application Active Directory (ADAM)

Le système nécessite un compte utilisateur pour lire les informations d'objet ADAM (Active Directory Application Mode) importées dans l'instance d'application.

Créez le compte à l'aide de l'une des méthodes suivantes :

- Créez un compte utilisateur ADAM local et attribuez-lui un mot de passe et des autorisations.
- Affectez une autorisation à un Windows compte de domaine sur la partition ADAM.
- Utilisez un compte `userProxy` .

Lorsque vous utilisez ADAM comme source LDAP, vous devez spécifier le nom distinct complet (FQDN) du compte ADAM dans le champ **Nom distinct de connexion** du serveur LDAP de l'instance.

Information associée

ADAM (Active Directory Application Mode)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Tester les connexions LDAPS

Testez les connexions LDAPS. Il existe deux connexions de console, l'une pour les certificats d'ordinateur local et l'autre pour les certificats de services informatiques locaux sur le nouveau service ADAM.

Avant de commencer

Rôle requis : admin

Procédure

1. Exécutez `LDP.exe` à partir du dossier d'installation d'ADAM c :\windows\adam.
   Vérifiez que la version ADAM est sélectionnée, car il ne s'agit pas du client LDP standard Windows .
2. Ouvrez une nouvelle connexion à l'aide du menu **Connexion/Connexion** .
   Le nom du serveur doit correspondre au CN attribué au certificat.
3. Entrez le **port LDAPS** et cochez la case **SSL** .
   Les résultats d'une connexion réussie sont des informations générales sur le serveur et aucune erreur.
4. Lier (se connecter) au service.
   Pour répliquer des connexions de client LDAP classiques, sélectionnez l'option Liaison simple. Entrez un nom unique d'utilisateur ADAM ou `de userProxy` valide dans le champ d'utilisateur et le mot de passe associé.
   Si vous voyez un message de retour indiquant « Authentifié en tant que :... ». vous êtes alors connecté avec succès à l'aide de LDAPS.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Utiliser ADAMSync pour renseigner ADAM

Les administrateurs utilisent MS ADAMSync pour renseigner les répertoires LDAP qui utilisent MS ADAM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Ce document suppose que vous avez au moins un niveau de compréhension de base de Microsoft Windows Server, Active Directory et ADAM et que vous disposez déjà d'une instance fonctionnelle ADAM (Active Directory Application Mode) avec une partition.

Ce sont des exemples de procédures. En raison de sa complexité et du fait qu'il s'exécute dans votre environnement, nous ne pouvons pas offrir d'assistance directe. Nous vous recommandons de travailler avec Microsoft un consultant si vous rencontrez des Microsoft problèmes.

Une fois qu'ADAM a été installé et que la première partition a été créée, vous pouvez la remplir d'objets.

Les options suivantes sont disponibles :

- Création manuelle d'objets à l'aide d'une interface graphique ou de scripts. Cette option est inefficace et lente.
- Intégrez Active Directory à l'aide du serveur d'informations d'intégration Microsoft . En fin de compte, cette option offre le plus de flexibilité et de fonctionnalités, mais nécessite des configurations avancées. Il existe une version gratuite de MIIS compatible avec Active Directory, ADAM etMicrosoft les listes d'adresses globales d'Exchange. À moins que vous n'ayez déjà de l'expérience avec MIIS, nous vous conseillons de ne pas essayer d'implémenter un nouvel environnement uniquement pour l'intégration LDAP.
- Utilisez ADAMSync, un outil de synchronisation fourni Microsoft avec ADAM. C'est l'option qui est expliquée ici.

Définir les comptes utilisateur ADAM

Définissez les comptes d'utilisateurs dans ADAM. Un compte utilisateur est utilisé pour l'instance à laquelle se connecter et l'autre compte utilisateur est pour ADAMSync.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ces comptes peuvent être des objets ADAM User locaux, des objets UserProxy ou un compte Windows d'un domaine approuvé.

Le *`ADAM User`* compte nécessite un accès en lecture seule à la structure de répertoire que vous importez dans votre instance. La meilleure façon d'y parvenir est d'ajouter le compte à l'attribut de membre dans le groupe de lecteurs qui se trouve dans cn=roles,dc=myCompany,dc=adam.

Les nouveaux comptes utilisateur ADAM sont désactivés par défaut. Vous devrez activer les nouveaux comptes et définir un mot de passe.

Procédure

1. Activez les utilisateurs en changeant l'attribut msDS-UserAccountDisabled en FAUX.
2. Cliquez avec le bouton droit sur l'objet utilisateur et réinitialisez le mot de passe.
3. Testez les nouveaux comptes à l'aide de LDP tel que défini dans ADAM (Active Directory Application Mode) pour vous assurer qu'ils peuvent se connecter.
   Utiliser le **LDAP** > **Vue/arborescence** , en laissant le DN de base vide pour vous assurer que vous pouvez afficher les objets dans le répertoire à l'aide des nouveaux comptes. La configuration, le schéma et la partition de domaine doivent être visibles dans le panneau de gauche. Traversez la partition de domaine. Si vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

utilisez un nouveau compte ADAM local, il affichera 'No Children', ce qui signifie que vous n'avez pas d'accès en lecture aux objets. Vérifiez les appartenances au groupe de configuration et effectuez un nouveau test.

ADAMSync utilise le compte pour gérer les *ADAMSync User* objets de la partition ADAM. Ce compte nécessite des droits de niveau administrateur puisqu'il crée, met à jour et supprime des objets ADAM.

ADAMSync utilise le *ADAMSync AD* compte pour lire les objets AD qui seront synchronisés avec ADAM.

Configurer ADAMSync

ADAMSync est inclus avec Windows le serveur 2003 R2. Téléchargez et installez ADAMSync si vous utilisez un autre système d'exploitation.

Extension du schéma

Le schéma ADAM doit être étendu pour prendre en charge ADAMSync.

1. Exécutez la commande suivante à partir de c :\windows\adam pour importer les extensions de schéma ADAMSync. Vous devrez peut-être modifier le server :port et ajouter des informations d'identification si l'utilisateur actuel n'y a pas accès. Voir le fichier AdamSyncMetadata.ldf pour plus de détails.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

2. Faites de même avec MS-AdamSchemaW2k3.ldf pour prendre en charge les attributs Windows 2003.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

Changements de schéma recommandés

Voici quelques modifications de schéma supplémentaires que nous recommandons.

1. Ouvrez une nouvelle console MMC et ajoutez le composant enfichable ADAM Schema.
2. Connectez-vous à l'instance ADAM.
3. Développez le dossier Classes et localisez la classe userProxy, ouvrez **Propriétés**.
4. Vérifiez les attributs facultatifs suivants dans l'onglet Attributs, ajoutez-en ceux qui n'existent pas déjà.
   - company
   - département
   - givenNane
   - courrier
   - physicalDeliveryOfficeName
   - sAMAccountName
   - Sn
   - Numéro de téléphone
   - Titre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- userAccountControl
- userPrincipalName

5. Redémarrez le service ADAM pour activer les nouveaux paramètres.

Installer le fichier de configuration ADAM

Installez le fichier de configuration ADAM via la ligne de commande Windows.

Avant de commencer
Rôle requis : admin

Procédure

1. Installez le fichier de configuration.

```
C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML
```

2. Exécutez le fichier de synchronisation à journaliser sur la console.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Consultez les résultats à l'aide de la console ADSIEdit.
   Vous devriez voir les nouveaux objets et attributs qui ont été créés par ADAMSync.
4. Exécutez ldap pour tester l'authentification UserProxy.
   Automatisation du processus de synchronisation

   Configurez le processus de synchronisation en tant que Windows tâche planifiée. Vous devez soit fournir les informations d'identification dans le fichier de configuration, soit dans la ligne de commande, soit exécuter la tâche planifiée avec un compte qui y a accès.

   Notes spéciales

   - Vous pouvez créer plusieurs fichiers de configuration et travaux planifiés pour synchroniser ADAM à partir de plusieurs sources.

     Cet exemple importe l'attribut sAMAccountName qui peut être utilisé comme connexion à l'application. Si vous voulez synchroniser la source, vous devez vous assurer que vous disposez d'une valeur d'attribut unique qui peut être utilisée pour les informations d'identification de connexion. sAMAccountName est garanti être unique au sein d'un domaine, mais pas dans plusieurs domaines.

   - Si vous utilisez Microsoft Exchange, nous vous recommandons d'exclure les objets cn=SystemMailbox* dans le cadre de la configuration objet-filtre.

Exemples de fichiers de configuration ADAM

Toutes les configurations d'ADAMSync sont stockées dans des fichiers XML.

Fichier de configuration par défaut avec commentaires

Un fichier de configuration par défaut appelé MS-AdamSyncConf.xml inclus dans l'installation d'ADAMSync. Faites une copie de ce fichier afin d'avoir un exemple de base auquel vous référer à l'avenir. Cet exemple est le fichier de configuration par défaut avec des commentaires ajoutés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;
  <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD -->;
<!-- if not used, the current user will be used  -->;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
  <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
  <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
   <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users -->;
<!-- need to review results to see if you should modify this filter -->;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account -->;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;sAMAccountName</include>;
   </attributes>;
  </query>;
<!-- map for user-to-userproxy object types -->;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
  <authoritative-adam-instance>;</authoritative-adam-instance>;
  <configuration-file-guid>;</configuration-file-guid>;
  <last-sync-attempt-time>;</last-sync-attempt-time>;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
 </synchronizer-state>;
</doc>;
```

Fichier de configuration des filtres LDAP

Vous pouvez fournir n'importe quel niveau de filtrage dans la valeur object-filter du fichier de configuration. Utilisez la syntaxe de requête LDAP standard avec les caractères d'échappement XML suivants à la place des opérateurs standard.

- ET = « & » remplacer par &
- OR = « | » (ligne verticale) remplacer par |
- NOT = « ! » remplacer par !

Fichier de configuration de référence

Voici un fichier de configuration réel qui peut être référencé comme exemple.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
  <security-mode>;object</security-mode>;
  <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
  <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
  <query>;
   <base-dn>;dc=service-now,dc=com</base-dn>;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;userAccountControl</include>;
   </attributes>;
  </query>;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 <aging>;
  <frequency>;0</frequency>;
  <num-objects>;0</num-objects>;
 </aging>;
 <schtasks-cmd>;</schtasks-cmd>;
</schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

Configurer Microsoft Active Directory pour une communication LDAPS sécurisée

Utilisez des paires de certificats pour activer les communications LDAPS Microsoft Active Directory (AD).

Remarque :
Ces procédures ont été conçues et testées à l'aide de Windows 2003 R2 Standard Edition et fonctionnent avec toutes les versions de Windows 2003.

La communication LDAPS sécurisée (LDAPS) est similaire à la communication SSL (HTTPS) en ce sens que les deux chiffrent les données entre les serveurs et les clients. Pour ce faire, le serveur et les clients partagent des informations communes à l'aide de paires de certificats. Le serveur détient le certificat de clé privée et les clients le certificat de clé publique. Ces certificats sont requis pour activer les communications LDAPS Microsoft Active Directory (AD).

Pour configurer LDAPS pour Active Directory, vous devez :

- Assurez-vous que le domaine Active Directory est configuré et que l'instance est en mesure de se connecter au serveur Active Directory via le pare-feu.
- Vérifiez qu'il existe une autorité de certification (CA) qui peut émettre un certificat pour le contrôleur de domaine (DC). Si vous n'avez pas encore d'infrastructure d'autorité de certification, deux options s'offrent à vous.
  - Configurer une autorité de certification autonome pour émettre le certificat
  - Demander un certificat de tiers
- Si vous avez déjà une autorité de certification en place, vous pouvez générer un certificat à partir d'une autorité de certification interne.

Tous les certificats ont une date d'expiration définie qui peut être consultée dans les propriétés du certificat. Si le certificat expire, tout le trafic LDAPS échoue et vos

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

utilisateurs ne peuvent plus se connecter à l'instance. Pour résoudre ce problème, un nouveau certificat doit être émis et installé sur votre instance.

La date d'expiration par défaut des certificats Microsoft CA est d'un an. Les certificats d'autorité de certification externes sont généralement achetés par tranches d'un an. Notez l'expiration de votre certificat ou utilisez la fonction de notification d'expiration de l'application (située dans **Système LDAP** > **Certificats**). Assurez-vous d'avoir un nouveau certificat prêt avant l'expiration de l'ancien. Cela vous laisse le temps d'installer et de tester le nouveau certificat avant l'expiration de l'ancien.

Configurer une autorité de certification autonome pour Active Directory

La première étape pour configurer Microsoft Active Directory pour l'accès SSL consiste à configurer une autorité de certification (CA) autonome.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ne vous inquiétez pas de l'utilisation des ressources supplémentaires, car les deux services requis (IIS et CA) peuvent être désactivés après l'émission du ou des certificats.

Procédure

1. Installez Internet Information Server (IIS).
2. Installez les services de l'autorité de certification en mode autonome.
3. Vérifiez que l'application Web Services de certificats est installée et active.

Que faire ensuite
À l'aide de la console du Gestionnaire IIS, développez l'ordinateur local et sélectionnez *Sites Web*. L'état du **site Web par défaut** doit être *En cours d'exécution*. Vous devriez également voir une demande *CertSrv* répertoriée sous le **site Web par défaut**. Si le site n'est pas en cours d'exécution ou si l'application est manquante, vous devez résoudre le problème avant de continuer.

Générer un certificat à partir d'une autorité de certification interne

Lorsque vous configurez Microsoft Active Directory pour l'accès SSL, vous devez générer un certificat interne et demander le certificat externe.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ces étapes s'appliquent aux services Microsoft CA. Si vous disposez d'une autre plateforme CA interne, consultez votre administrateur CA local pour obtenir de l'aide.

Procédure

1. À partir du contrôleur de domaine (DC) pour lequel vous souhaitez créer un certificat, accédez à `http://localhost/certsrv` ou spécifiez le nom du serveur CA s'il se trouve sur un serveur distant.
2. À partir de la page d'accueil, cliquez sur **Demander un certificat** et sélectionnez *Demande de certificat avancée*.
3. Sur la page Advanced Certificate Request (Demande de certificat avancé), sélectionnez **Créer** et soumettez une demande à cette autorité de certification.
4. Complétez la demande de certificat avancé comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de demande de certificat avancé

Champ	Entrée
Nom	Nom de domaine complet (FQDN) du collecteur de données qui demande le certificat.
Courriel	L'adresse électronique de la personne responsable du certificat.
Société	Nom de votre société.
Paramètres des options clés	
Créer un jeu de clés	Sélectionnez-le.
Demande de signature de certificat	Fournisseur de cryptographie Microsoft RSA Shannel.
Utilisation de la clé	Échanger.
Taille de la clé	1024 est recommandé. L'instance prend en charge jusqu'à 2048.
Nom du conteneur de clés automatique	Sélectionnez-le.
Stocker le certificat dans la banque de certificats de l'ordinateur local	Sélectionnez-le.

5. Cliquez sur **Envoyer**.
   Vous êtes dirigé vers une page qui fournit votre **ID de demande**, notez-le.
6. Pour traiter la demande en attente, procédez comme suit :
   a. Ouvrez la console de gestion de l'autorité de certification.
   b. Développez le nœud du serveur et sélectionnez **Demandes en attente**.
   c. Localisez l'ID de demande de la demande que vous venez de soumettre, cliquez avec le bouton droit de la souris et sélectionnez *Toutes les tâches/le problème pour approuver la demande et émettre le certificat*.
7. Pour récupérer le certificat émis, procédez comme suit :
   a. À partir du contrôleur de domaine à partir duquel vous avez effectué la demande, accédez à `http://localhost/certsrv` ou spécifiez le nom du serveur CA s'il se trouve sur un serveur distant.
   b. Sélectionnez `Afficher l'état d'une demande de certificat en attente`.
   c. Sélectionnez le lien vers le nouveau certificat.
   d. Sélectionnez le lien pour **installer ce certificat**.

Que faire ensuite

Vous devez demander un certificat tiers. Les certificats auprès d'autorités de certification externes peuvent être achetés pour aussi peu que 30 $ par an. Pour connaître les procédures détaillées sur la demande d'un certificat auprès d'une autorité de certification externe, consultez l'article Microsoft 321051 . Une fois reçu, installé et testé, suivez la procédure d'exportation.

Tester la connectivité LDAPS localement

Testez la connectivité LDAPS après l'installation des certificats internes et tiers lorsque vous configurez Microsoft Active Directory pour l'accès SSL.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Assurez-vous que les outils de support Windows sont installés sur le contrôleur de domaine (DC).
   Le programme d'installation des outils de support (suptools.msi) se trouve dans le répertoire `\Support\Tools` de votre CD Windows Server.
2. Accédez à la **Début** > **Tous les programmes** > **Outils de support Windows** > **Ligne de commande**.
   Sur la ligne de commande, saisissez `ldp` pour démarrer l'outil .
3. Dans la fenêtre *LDP* , sélectionnez **Connexion** > **Connect** et fournissez le FQDN local et le numéro de port (636).
   Sélectionnez également le *SSL*.
   En cas de réussite, une fenêtre affiche et répertorie les informations relatives à la connexion SSL Active Directory. Si la connexion échoue, essayez de redémarrer votre système et répétez cette procédure.

Exporter le certificat de clé publique pour approuver le certificat LDAP

Exportez le certificat de clé publique et importez-le dans l'application lorsque vous configurez Microsoft Active Directory pour l'accès SSL.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Si votre autorité de certification n'est pas un fournisseur tiers approuvé, vous devez exporter le certificat pour l'autorité de certification émettrice afin que nous puissions lui faire confiance et, par association, approuver le certificat du serveur LDAP. Pour les utilisateurs de MS Certificate Services, vous pouvez afficher le chemin d'accès du certificat en affichant le certificat dans la console utilisée pour exporter ; sélectionnez l'onglet **Chemin d'accès au certificat** . Vous devez exporter tous les certificats de la chaîne. Vous pouvez trouver le certificat CA dans le même dossier que le certificat LDAP en recherchant le nom dans le chemin d'accès du certificat. Soumettez tous les certificats pour importation dans votre instance.

Procédure

1. À partir d'une console MMC actuelle ou nouvelle, ajoutez le composant logiciel enfichable Certificat (ordinateur local).
2. Ouvrez le dossier `Personnel/Certificats` .
3. Localisez le nouveau certificat.
   La colonne Délivré à affiche le nom de domaine complet du contrôleur de domaine.
4. Cliquez avec le bouton droit sur le certificat et sélectionnez *Toutes les tâches/Exporter*.
5. Exporter au format DER ou Base-64.
   Nommez le fichier en utilisant le format `MyCompany.cer`. Il s'agit du certificat de clé publique qui doit être utilisé sur l'instance pour communiquer en toute sécurité avec votre contrôleur de domaine.
6. Testez LDAPS localement avant de soumettre le certificat à l'instance.

Que faire ensuite

Une fois cette procédure terminée, importez le certificat de clé publique dans l'application.
Voir Installer le certificat SSL LDAP X.509 pour charger le certificat dans l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du catalogue LDAP global

Un contrôleur de domaine peut se voir accorder le rôle de catalogue global (GC). Le rôle Catalogue global (GC) est un répertoire compatible LDAP consistant en une représentation partielle de chaque objet de chaque domaine au sein d'une forêt.

Les administrateurs configurent Active Directory pour héberger les informations de répertoire LDAP (Lightweight Directory Access Protocol) à l'aide de l'une des méthodes d'hébergement suivantes.

- La méthode courante d'hébergement des informations de l'annuaire LDAP consiste à utiliser le LDAP ou LDAPS (LDAP sécurisé) par défaut sur les ports 389 ou 636. Ces ports LDAP standard existent toujours sur un contrôleur de domaine (DC) et sont rarement modifiés. L'accès à cette partition de répertoire permet d'accéder à tous les objets du domaine hébergé sur le contrôleur de domaine. Il n'y a aucun moyen d'accéder aux objets d'autres domaines à l'aide de cette méthode.
- Un contrôleur de domaine peut également se voir attribuer le rôle de catalogue global (GC). Le rôle Catalogue global (GC) est un répertoire compatible LDAP consistant en une représentation partielle de chaque objet de chaque domaine de la forêt. Ce répertoire LDAP est accessible sur le port 3268, LDAPS sur le port 3269. Les exigences en matière de certificat LDAPS et des ports LDAP par défaut sont les mêmes.

Dépendances LDAP du catalogue global

- Le contrôleur de domaine auquel votre instance se connecte doit avoir le rôle Catalogue global activé.
- Les règles de pare-feu doivent autoriser le trafic entrant vers le contrôleur de domaine sur le port 3268 (LDAP) ou 3269 (LDAPS).

Notes spéciales

- Tous les attributs ne sont pas répliqués sur la partition GC. Les attributs communs tels que le prénom, le nom, l'adresse e-mail, le numéro de téléphone, la description et l'adresse sont inclus. Des attributs supplémentaires peuvent être ajoutés au GC, mais doivent être limités pour minimiser l'impact sur le trafic de réplication de la forêt.
- Les intégrations LDAP standard utilisent généralement sAMAccountName comme ID d'utilisateur de l'instance et comme clé de fusion dans la carte d'importation LDAP, car celui-ci est garanti comme unique au sein d'un domaine. Cet attribut n'est plus unique lors de l'affichage d'une forêt entière de domaines. Un nouvel attribut unique doit être identifié en tant que UserID et clé de fusion. Ceux-ci n'ont pas besoin d'être le même attribut et peuvent varier en fonction de la conception de votre forêt. Consultez votre administrateur Active Directory. En règle générale, le userPrinicpalName est un attribut unique dans tous les domaines, mais ce n'est peut-être pas un nom convivial pour se connecter, mais il peut être utilisé pour l'identificateur unique sur les importations. L'adresse e-mail est un attribut commun utilisé pour le UserID. Ces décisions ont un impact sur les propriétés LDAP et le mappage LDAP.
- La valeur utilisée pour la clé de fusion sur la carte d'importation LDAP doit être unique et exister sur chaque objet importé. S'il n'est pas unique ou n'existe pas, les enregistrements incorrects sont mis à jour avec les changements.
- Si vous avez déjà une intégration LDAP et que vous souhaitez la changer en GC, changez la clé de fusion d'importation. Les nouvelles valeurs de clé doivent être importées avant de pouvoir modifier la clé de fusion.
- Si vous apportez des modifications à votre intégration LDAP qui interrompent votre intégration, votre première étape consiste à rétablir ces modifications. Après cela, contactez Service client et assistance des informations complètes sur ce que vous essayez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modification mineure du schéma OpenLDAP

Dans les systèmes OpenLDAP 2.3 qui utilisent le back-bdb (Berkley backend), les administrateurs apportent une modification mineure à leur schéma pour faciliter l'intégration.

⚠ Avertissement :
La personnalisation décrite ici a été développée pour une utilisation dans des instances spécifiques, et n'est pas prise en charge par Now Support. Cette méthode est fournie telle quelle et doit être testée rigoureusement avant d'être implémentée. Publiez toutes les questions et commentaires concernant cette personnalisation dans notre forum communautaire.

Dans OpenLDAP 2.3, back-bdb a un support limité pour l'indexation des inégalités (classement). Elle n'est implémentée que pour la syntaxe generalizedTime et ChangeSequenceNumber. Il ne peut pas être pris en charge sur une syntaxe qui prend en charge les sous-chaînes. Les filtres de recherche contenant des inégalités sont traités à l'aide de l'indice de présence.

Nous recommandons de créer un attribut personnalisé à cet effet, au lieu de modifier ce qui est déjà indexé ou présent dans le schéma (par exemple, *`servnowid`*).

Modifier le schéma OpenLDAP

Modifiez le schéma OpenLDAP. Ces étapes détaillent une modification du schéma d'OpenLDAP 2.3 fournie par l'un de nos clients qui l'a aidé à s'intégrer à son instance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

⚠ Avertissement :
La personnalisation décrite ici a été développée pour une utilisation dans des instances spécifiques, et n'est pas prise en charge par Now Support. Cette méthode est fournie telle quelle et doit être testée rigoureusement avant d'être implémentée. Publiez toutes les questions et commentaires concernant cette personnalisation dans notre forum communautaire.

Pour modifier le schéma OpenLDAP afin de l'intégrer à l'instance :

Procédure

1. Créez un attribut personnalisé.

   Example

```
attribute ( 1.3.6.1.4.1.3403000.2.1.8

    NAME 'servnowid'
 ORDERING caseIgnoreOrderingMatch
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

2. Inclure l'attribut dans l'OID objectclass sélectionné.

   Example

```
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
 MAY ( uniqid $ unixid $ servnowid ) )
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans OpenLDAP 2.3, vous pouvez modifier dynamiquement les configurations du serveur, mais vous ne pouvez qu'étendre le schéma. Vous ne pouvez pas modifier ou supprimer le schéma existant. Au lieu de créer une autre classe d'objet pour cet attribut dans la configuration dynamique, utilisez le fichier de configuration statique, slapd.conf.

3. Dans slapd.conf, incluez l'indexation du nouvel attribut dans la section bdb de votre backend de base de données principal.

   Example

   ```
   database bdb (configs here) ....

   index servnowid pres

   (other indexes here) .....
   ```

4. En tant qu'élément root, exécutez slapindex pour indexer cet attribut afin de le rendre disponible dans les filtres de recherche.
   Assurez-vous que le démon OpenLDAP n'est pas en cours d'exécution ou en mode lecture seule avant de démarrer slapindex.

Suppressions LDAP d'enregistrements

Par défaut, l'instance ne supprime aucune entrée après leur disparition de LDAP.

La suppression d'une entrée, également appelée *enregistrement*, supprime également tout l'historique et les références à l'entrée supprimée.

Par exemple, les éléments de configuration (CI), les accords SLA, les licences de logiciels, les bons de commande et les entrées de catalogue de services ont tous une référence au département. Si un département est supprimé, l'intégration efface toutes les références au département. De plus, la suppression d'un utilisateur entraîne la perte de tout l'historique de ce qu'il a fait.

Décidez de conserver ou Delete all records from a table en fonction des besoins de votre organisation.

Sessions simultanées limites

Vous pouvez limiter le nombre de sessions interactives simultanées pour un utilisateur ou un rôle sur une instance sur tous les nœuds.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Explorer



Découvrez les fonctionnalités et la valeur commerciale des sessions simultanées limitées.

Activer



Découvrez comment activer le nombre limite de sessions simultanées.

Ensemble



Définissez la limite de sessions simultanées pour un utilisateur ou un rôle.

Désactiver



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer le nombre limite de sessions simultanées

Vous pouvez limiter le nombre de sessions interactives simultanées pour un utilisateur ou un rôle sur une instance sur tous les nœuds.

Les sessions interactives simultanées font référence au nombre de sessions actives qu'un utilisateur peut avoir actives par ServiceNow instance. Une session d'instance active se produit à chaque nouvelle connexion à une instance spécifique ServiceNow . Par défaut, il n'y a aucune limite au nombre de sessions d'instance actives qu'un utilisateur peut avoir.

Avec la version Jakarta, vous pouvez limiter le nombre de sessions simultanées actives par utilisateur. Lorsque l'utilisateur se connecte après avoir atteint le nombre maximal de sessions actives, la session active la plus ancienne se termine et une nouvelle session interactive devient active. Si un utilisateur tente d'accéder à une session fermée via un navigateur, il est redirigé vers la page de connexion.

Remarque :
Le module **d'extension Limite de sessions simultanées** doit être actif pour activer une limite de session maximale. Les limites sont définies via la propriété glide.authenticate.max.concurrent.interactive.sessions. Une valeur limite maximale s'applique à tout utilisateur ou rôle pour lequel la propriété limite est active. Un utilisateur ou un rôle connecté à l'utilisateur doit avoir la valeur limit_concurrent_sessions définie sur vrai pour que la limite de sessions soit lancée. Pour la version Jakarta, cette fonctionnalité ne prend pas en charge les sessions créées via l'application mobile native ou les mécanismes non interactifs.

Un cas d'utilisation typique si une session simultanée maximale de 1 est définie :

1. L'utilisateur accède à l'instance initiale ServiceNow via Chrome.
2. Une fois que l'utilisateur s'est connecté avec succès, ServiceNow crée la session 1 (S1) pour l'utilisateur.
3. L'utilisateur décide d'initier un autre accès à l'instance ServiceNow via Firefox.
4. Une fois que l'utilisateur s'est connecté avec succès, ServiceNow crée la session 2 (S2) pour l'utilisateur.
5. Étant donné que l'utilisateur dispose d'une limite maximale de sessions simultanées de 1, la session S1 s'invalide lorsque S2 est créé.
6. Lorsque l'utilisateur revient via Chrome pour accéder à l'instance S1 ServiceNow , il est redirigé vers la page de connexion, car S1 n'est pas valide.

Les limites de ServiceNow session simultanée fonctionnent avec tous les mécanismes d'authentification : SAML, LDAP et authentification de base de données locale. Il fonctionne également avec l'authentification multifacteur et tous les mécanismes d'authentification interactifs ServiceNow . La source de la session est visible via la table **sys_user_session** , sous la colonne **Type**. Les valeurs peuvent être :

- Navigateur Web
- Navigateur mobile
- ServiceNow Application mobile
- Non interactif (SOAP, WSDL, OAuth)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer et configurer le module d'extension de limite de sessions simultanées

Vous pouvez activer le module d'extension Limite de sessions simultanées (com.glide.limit.concurrent.sessions) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**.
2. Recherchez et cliquez sur le module d'extension Limite de sessions simultanées.
3. Dans le formulaire Module d'extension système, examinez les détails du module d'extension, puis cliquez sur le lien connexe **Activer/mettre à niveau** .
4. Cliquer sur **Activer**.
5. Pour activer cette fonctionnalité et définir une limite maximale de sessions simultanées, accédez à l'onglet **Fichiers de module d'extension** , recherchez les propriétés suivantes et modifiez les valeurs de réglage.

Option	Description
glide.authenticate.limit.concurrent.interactive-.sessions	Vous pouvez activer la possibilité de limiter les sessions simultanées en définissant la valeur **sur Vrai**. Par défaut, cette propriété est définie sur **Faux**, ce qui signifie qu'il n'y a pas de limite au nombre de sessions interactives qu'un utilisateur peut avoir actives. **Remarque :** Pour désactiver cette fonctionnalité, redéfinissez cette propriété sur **Faux**.
glide.authenticate.max.sessions.interactives-.concurrentes	Vous pouvez définir le nombre maximal de sessions interactives actives simultanées qu'un utilisateur peut avoir sur l'instance sur tous les nœuds.

6. **Facultatif :** Vous pouvez également modifier les propriétés suivantes, si nécessaire.

Option	Description
glide.authenticate.session.types.to.limit.concur-rency	Cette propriété limite les types de sessions. Par défaut, seules les sessions de navigateur Web ont une limite. Les types de sessions sont les suivants : ○ Navigateur Web (1) ○ Navigateur mobile (2) ○ ServiceNow Application mobile (3) ○ Non interactif (10) Vous pouvez configurer et définir la valeur sur « 1 » pour le navigateur Web, « 2 » pour le navigateur mobile ou « 1,2 » pour les deux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Seules les sessions de navigateur Web et mobile peuvent avoir une limite. Il n'y a aucune limite pour les sessions qui proviennent de l'application mobile ou les ServiceNow sessions non interactives.
glide.authenticate.limit.concurrent.sessions-.across.all.nodes	Cette propriété limite la limite de sessions simultanées par nœud au lieu de les restreindre dans tous les nœuds d'une ServiceNow instance. Par défaut, la valeur est définie sur vrai, ce qui limite les sessions utilisateur sur tous les nœuds. Si la propriété est définie sur false, seules les sessions sur ce nœud et non celles sur les autres nœuds sont soumises à la limite.

7. Cliquez sur **Mettre à jour** pour appliquer les paramètres.

Que faire ensuite

Définir une limite de sessions simultanées par utilisateur ou rôle.

Information associée

Liste des modules d'extension (Yokohama)

Définir une limite de sessions simultanées par utilisateur ou rôle

Vous pouvez définir une limite de session simultanée sur un utilisateur spécifique ou sur un rôle particulier.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs** ou **Administration utilisateurs** > **Rôles**.
2. Sélectionnez un utilisateur ou un rôle pour lequel vous souhaitez définir une limite de session simultanée, cochez la case **Limiter les sessions simultanées** , puis cliquez sur **Mettre à jour**.
   L'utilisateur ou le rôle a une limite quant au nombre de sessions simultanées pouvant être ouvertes simultanément.

Désactiver une limite de session simultanée par utilisateur ou rôle

Vous pouvez désactiver une limite de session simultanée sur un utilisateur spécifique ou sur un rôle particulier.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs** ou **Administration utilisateurs** > **Rôles**.
2. Sélectionnez un utilisateur ou un rôle pour lequel vous souhaitez désactiver une limite de sessions simultanées, décochez la case **Limiter les sessions simultanées** , puis cliquez sur **Mettre à jour**. L'utilisateur ou le rôle n'est pas soumis à une limite de nombre de sessions simultanées pouvant être ouvertes simultanément.

Authentification locale

Utilisez ServiceNow® l'authentification locale pour sécuriser la connexion des utilisateurs sur un appareil local.

L'authentification locale est une méthode de vérification de l'identité d'un utilisateur sur un appareil local. Elle utilise les caractéristiques uniques ou les informations d'identification possédées par l'utilisateur pour valider la connexion de l'utilisateur.

Utilisez ServiceNow® les fonctionnalités d'authentification locale de pour accéder en toute sécurité à l'instance ServiceNow® sur vos appareils locaux.

Sécurité de la connexion et de l'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Configurer la sécurité de votre connexion



Comprendre comment configurer la sécurité des connexions.

Définir des scénarios de connexion



Définissez les scénarios de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réinitialisation du mot de passe



En savoir plus sur les réinitialisations du mot de passe de connexion.

Traduction automatique

Explorer la sécurité de la connexion et de l'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Options de sécurité

Vous pouvez contrôler plusieurs aspects de la sécurité de connexion et d'authentification des utilisateurs :

Fonctionnalité	Description	Rubriques connexes
Contrôles de connexion et de déconnexion	Contrôlez plusieurs dimensions du processus de connexion et de déconnexion des utilisateurs, telles que la spécification d'une page de destination à laquelle l'utilisateur s'affiche lorsqu'il se connecte, et contrôlez la façon dont les utilisateurs se déconnectent.	• Définir des scénarios de connexion • Configurer l'invite de confirmation de déconnexion • Sorties d'installation • Spécifier le verrouillage en

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description	Rubriques connexes
		cas d'échec des tentatives de connexion
Sécurité de l'authentification	Contrôlez le processus de réinitialisation du mot de passe et des fonctionnalités telles que l'option Se souvenir de moi. Vous pouvez également utiliser des contrôles basés sur l'adresse IP pour accéder à l'instance et implémenter une valeur de circonstance à utiliser avec l'authentification synthèse d'authentification unique.	• Configurez votre politique de mot de passe • Réinitialisation du mot de passe • Mémoriser mon nom • Authentification basée sur la plage IP • Implémenter une valeur de circonstance

Définir des scénarios de connexion

Vous pouvez diriger tous les utilisateurs vers la même page après la connexion.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lorsque les utilisateurs se connectent directement à une instance, par exemple en accédant à http://{instance_name}.service-now.com/, le système effectue les opérations suivantes :

1. Accède à la valeur dans la propriété `glide.entry.page.script`. La valeur par défaut de la propriété est dérivée d'un include de script nommé *CMSEntryPage*.
2. Dirige l'utilisateur vers la page de connexion de l'instance si la page d'entrée nécessite une connexion.
3. Applique les règles de connexion, le cas échéant, à l'utilisateur.

Pour forcer le système à diriger tous les utilisateurs vers la même page après la connexion :

Procédure

1. Accédez à la **Tous** > **Gestion du contenu** > **Configuration** > **Page de configuration**.
2. Sélectionnez une valeur pour le champ *Page de connexion* ou créez une nouvelle page comme vous le souhaitez.

   Si cette page n'est pas la page par défaut du site, elle redirige toujours ici. S'il s'agit d'une page par défaut du site, elle applique les règles de connexion. Si cette valeur est nulle, le système utilise navpage.do comme page d'entrée. N'entrez pas de page de connexion ici ; Sinon, les utilisateurs doivent se connecter deux fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexion à une instance pour accéder à un enregistrement :

Lorsque les utilisateurs se connectent à une instance pour accéder à un enregistrement à l'aide de son identificateur unique global (sys_id), tel que http://{instance}.service-now.com/incident.do?sys_id={sys_id}, le système effectue les opérations suivantes :

a. Dirige l'utilisateur vers une page de connexion s'il n'est pas déjà connecté.

b. Dirige l'utilisateur vers l'enregistrement approprié s'il est autorisé à y accéder. Si l'utilisateur ne dispose pas des droits d'accès à l'enregistrement, un message de refus d'accès s'affiche.

Connexion au portail de services ou à un site CMS :

Lorsque les utilisateurs se connectent au Service Portal ou à un site CMS, tel que http://<instance>.service-now.com/site-name/page.do, le système effectue les opérations suivantes :

- S'il y a une valeur dans le champ *Page de connexion* sur le formulaire du portail de services ou du site CMS, il dirige l'utilisateur vers cette page de connexion et applique les règles de connexion, le cas échéant, à l'utilisateur.
- Si aucune page de connexion n'est spécifiée, l'utilisateur est dirigé vers la valeur du champ Page *d'accueil* du portail de services ou du formulaire du site CMS.

Connexion au portail de services ou à un site CMS pour accéder à un enregistrement :

Lorsque les utilisateurs se connectent au Portail de services ou à un site CMS pour accéder à un enregistrement, par exemple http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}, le système suit la même procédure et amène enfin l'utilisateur à l'enregistrement. Si l'utilisateur ne dispose pas des droits d'accès à l'enregistrement, un message de refus d'accès s'affiche.

Connexions et portail en libre-service employés

Le système effectue le suivi de la première page de démarrage à laquelle un utilisateur essaie d'accéder, même s'il souhaite se connecter au portail en libre-service employés.

Examinez les scénarios suivants.

Exemple 1 :

1. Un utilisateur n'est pas connecté et tente alors d'accéder à un enregistrement à l'aide d'un ID système spécifique dans l'URL.
2. Le système redirige l'utilisateur vers la page de connexion.
3. Plutôt que de se connecter, l'utilisateur essaie d'accéder à un autre site, tel que le portail Libre-service employés (/ess).
4. Le système redirige l'utilisateur vers la page de connexion.
5. L'utilisateur se connecte et est redirigé vers l'enregistrement auquel il essayait d'accéder en premier lieu plutôt que vers le portail en libre-service employés.

Exemple 2 :

1. Un utilisateur n'est pas connecté, puis tente d'accéder à un enregistrement à l'aide d'un ID SYS spécifique dans l'URL via le portail libre-service employés (/ess).
2. Le système redirige l'utilisateur vers la page de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Plutôt que de se connecter, l'utilisateur essaie d'accéder à un autre enregistrement via le portail en libre-service employés.
4. Le système redirige l'utilisateur vers la page de connexion.
5. L'utilisateur se connecte et est redirigé vers le premier enregistrement plutôt que vers le second.

Spécifier une page de destination de connexion

Par défaut, les utilisateurs voient leur page d'accueil lorsqu'ils se connectent. Vous pouvez spécifier une page de destination de connexion différente à l'aide d'une propriété système ou du système de gestion de contenu.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Pour spécifier une page de destination de connexion pour tous les utilisateurs, modifiez la valeur de la propriété dans la table sys_properties.

Procédure

1. Saisissez sys_properties.list dans le filtre de navigation.
2. Localisez la propriété système **glide.login.home** .
3. Dans le champ **Valeur** , saisissez le nom de la page que tous les utilisateurs voient en se connectant.

   Utilisez <nom de page>.do ; vous pouvez omettre la partie http ://"instance".service-now.com/ de l'URL . Pour déterminer le nom de page ou l'URL d'une page dans le système, vous pouvez pointer vers un lien. Certaines pages possibles sont welcome.do et incident.do.

   Pour spécifier une page de destination de tableau de bord, définissez la propriété sur $dashboards.do ?dashboard=<SYS_ID>. Remplacez <SYS_ID> par le sys_id du tableau de bord.

   Pour diriger les utilisateurs vers Service Portal, définissez la propriété sur /sp

   Remarque :
   Cette propriété s'applique à l'ensemble du système, sa définition affecte donc tous les utilisateurs. Pour définir une connexion spécifiquement destinée aux utilisateurs sans rôles, vous pouvez appliquer ces mêmes étapes et utiliser la propriété **glide.entry.loggedin.page_ess** .

   Vous pouvez également spécifier une page de destination de connexion avec le système de gestion de contenu.

Spécifier le verrouillage en cas d'échec des tentatives de connexion

Le système fournit des actions de script inactives qui vous permettent de spécifier le nombre d'échecs de tentatives de connexion avant qu'un compte utilisateur ne soit verrouillé et de réinitialiser le nombre après une connexion réussie.

Avant de commencer
Rôle requis : admin

Procédure

Accédez à la **Tous** > **Politique système** > **Actions des scripts** pour afficher ou activer les scripts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
À partir de la Kingston mise en production, après un zboot, les actions de script **SNC Vérification du verrouillage de l'utilisateur avec déverrouillage automatique** et **Effacement de l'utilisateur SNC** sont activées.

Pour en savoir plus sur les propriétés qui affectent les tentatives de connexion échouées, consultez Gestion des tentatives de connexion échouées (renforcement de la sécurité de l'instance) dans les paramètres de renforcement de la sécurité de l'instance.

Action des scripts	Description
Vérification du verrouillage de l'utilisateur SNC avec déverrouillage automatique	• Utilise la valeur de la propriété `glide.user.max_unlock_attempts` pour définir la limite des tentatives de connexion infructueuses. • Déverrouille le compte d'utilisateur après la période spécifiée pour la propriété `glide.user.unlock_timeout_in_mins` . Si aucune valeur n'est spécifiée, le système déverrouille le compte d'utilisateur après la période par défaut de 15 minutes.
Vérification du verrouillage de l'utilisateur SNC	Suit le nombre d'échecs de tentatives de connexion et verrouille le compte d'utilisateur après un nombre spécifié d'échecs de tentatives de connexion (par défaut : 5).
Effacement d'utilisateur SNC	Met à jour l'enregistrement utilisateur après une connexion réussie : réinitialise le nombre d'échecs de tentatives de connexion et met à jour la date de la dernière connexion.

Que faire ensuite
Chaque fois qu'un utilisateur tente de se connecter, l'action est enregistrée dans un journal des événements. Vous pouvez afficher un journal des tentatives de connexion infructueuses.

1. Accédez à la **Politique système** > **Journaux des événements**.
2. Filtre pour **login.failed** dans le champ **Nom** . Vous pouvez afficher le nom de la tentative de connexion, la date et l'adresse IP enregistrées pour la tentative.

Rendre les pages de l'interface utilisateur publiques ou privées

Vous pouvez rendre les pages publiques si vous souhaitez que vos utilisateurs voient les pages sans se connecter.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La plupart des pages ne sont visibles que par les utilisateurs connectés. Un nombre limité de pages sont publiques afin que les utilisateurs n'aient pas à se connecter pour les consulter, comme la page d'accueil, la page d'accueil et les pages de connexion et de déconnexion.

Avertissement :
Plusieurs pages publiques du système de base sont requises pour la fonctionnalité de nombreuses fonctionnalités. Ne désactivez pas les pages publiques du système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le filtre du navigateur d'application, tapez `sys_public.list`.
2. Cliquez sur **Nouveau**.
3. Dans la table sys_public, créez un enregistrement avec les valeurs suivantes.

Champ	Description
Page	Le nom de la page. Par exemple : $sp
Actif	Lorsque cette option est sélectionnée, la page est publiquement accessible. Désélectionnez l'option Actif lorsque vous souhaitez que la page soit privée.

4. Cliquez sur **Enregistrer**.
   En définissant actif sur vrai, la page est publique, de sorte que toute personne visitant `<instance_name>/sp` ou `<instance_name>/$sp.do` peut accéder à la page.

Exigences de complexité des mots de passe

Dans votre ServiceNow® instance, les mots de passe doivent répondre aux exigences de complexité.

Explorer



Découvrez les fonctionnalités et la valeur commerciale des exigences de complexité des mots de passe.

Activer



Découvrez comment activer les exigences de complexité du mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Configurez les critères de complexité du mot de passe.

Référence : caractères de mot de passe non pris en charge



Connaissez les caractères de mot de passe non pris en charge.

Traduction automatique

Explorer les exigences de complexité des mots de passe

Dans votre ServiceNow® instance, les mots de passe doivent répondre aux exigences de complexité.

Le paramètre de stratégie Exigences de complexité des mots de passe détermine si les mots de passe doivent respecter une série de directives en matière de mots de passe forts.

Les exigences de complexité des mots de passe sont appliquées lorsqu'un mot de passe est modifié ou créé.

Les exigences de complexité des mots de passe respectent et fonctionnent en fonction de ce qui suit :

- Si la `glide.apply.password_policy.on_login` propriété est activée, la vérification de la politique de mot de passe est appliquée à l'utilisateur pendant la connexion. Lors de la connexion, l'utilisateur doit respecter la politique de mot de passe et modifier le mot de passe de l'instance.
- Les exigences de la politique en matière de mots de passe sont basées sur le plan multilingue de base (BMP) qui contient des caractères pour toutes les langues modernes. ServiceNow les instances sont livrées avec des BMP d'environ 10 000 caractères.
- Les mots de passe dans les BMP autorisées peuvent être définis pour votre instance. Les mots de passe qui ne respectent pas ces BMP ne sont pas autorisés.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si nécessaire, vous pouvez exiger que les mots de passe soient changés régulièrement, au moins tous les 90 jours.

Conditions requises et personnages interdits

Pour activer un environnement réseau sécurisé, il est nécessaire que les utilisateurs utilisent des mots de passe forts qui incluent une combinaison de lettres, de chiffres et de symboles. Ces combinaisons aident à empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées pour deviner des mots de passe faibles.

Le mot de passe de votre instance doit répondre aux exigences suivantes :

- 8 caractères minimum.
- 100 caractères maximum.
- Contient des caractères minuscules et majuscules
- Contient des caractères spéciaux.
- Contient des chiffres.

Vous pouvez interdire une liste de mots de passe incorrects courants, tels que les suivants :

- Séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$ %^ », « aaaaa », etc.
- Nom de l'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que le siège social de la société, la ville, le pays, etc.
- Termes internes ou abréviations spécifiques à l'entreprise.
- Emojis.

Remarque :
Les caractères spécifiques à l'utilisateur, à la marque ou à la société qui ne peuvent pas être utilisés dans le mot de passe peuvent être configurés dans la page Politique de mot de passe ou Exclure le mot de passe.

Activer les politiques de mot de passe sur votre instance

Implémentez des contrôles de politique de mot de passe lors de la connexion. Forcer les utilisateurs à changer leur mot de passe si le mot de passe ne correspond pas aux critères de politique de mot de passe.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Le module d'extension Politique de mot de passe (com.glide.password_policy) est activé par défaut. La politique entre en vigueur lorsqu'un utilisateur modifie ou réinitialise le mot de passe.
Le champ **Force du mot de passe prédéfinie** est automatiquement défini sur **Fort par défaut**. Si vous souhaitez ajouter de nouveaux critères, vous pouvez effectuer la procédure suivante.

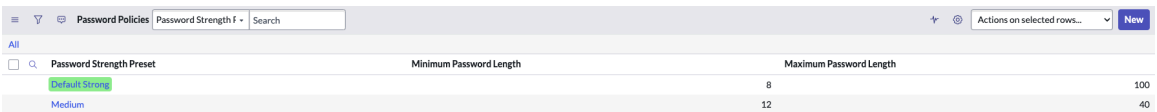
Si vous avez personnalisé votre instance via la sortie d'installation ou votre `ValidatePasswordStronger` propriété de banque `pwd_cred_store` d'identifiants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réinitialisation du mot de passe, consultez Propriétés de la politique de mot de passe pour savoir comment implémenter une stratégie de mot de passe pour votre instance.

Remarque :
La politique de mot de passe active est mise en surbrillance pour l'instance, comme indiqué.



Pour modifier la politique de mot de passe, accédez à **Tous** > **Réinitialisation du mot de passe** > **Banques d'informations d'identification**, sélectionnez les informations d'identification et modifiez le champ **Politique du mot de passe** pour l'entrée de politique requise.

Procédure

1. Accédez à la **Tous** > **Politique de mot de passe** > **Politiques de mot de passe**.
2. Cliquez sur **Nouveau**.
   Le formulaire Politique de mot de passe s'affiche.
3. Spécifiez le **nom** de votre politique de mot de passe.
4. Dans la section Critères de politique de mot de passe, sélectionnez l'un des paramètres prédéfinis suivants dans le champ **Force du mot de passe prédéfinie** .

   Remarque :
   La politique de mot de passe est appliquée en fonction du paramètre prédéfini sélectionné.

5. Renseignez les champs restants du formulaire.

Formulaire Politique de mot de passe

Champ	Description
Longueur minimale du mot de passe	Longueur minimale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**. Définissez ce champ sur un minimum de 8 à 10 caractères.
Longueur maximale du mot de passe	Longueur maximale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**. Définissez ce champ sur un maximum de 100 caractères.
Caractère(s) majuscule(s) minimum	Nombre minimum de caractères majuscules dans le mot de passe, de 0 à 10.
Caractère(s) minuscule(s) minimum	Nombre minimum de caractères minuscules dans le mot de passe, de 0 à 10.
Caractère(s) numérique(s) minimum	Nombre minimum de caractères dans le mot de passe, de 0 à 10.
Caractère(s) spécial(ux) minimum	Nombre minimum de caractères spéciaux dans le mot de passe, de 0 à 10.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Caractères spéciaux inclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez `$, !`, les utilisateurs ne peuvent utiliser que « $ » et « ! » comme caractères spéciaux dans le mot de passe. Aucun autre caractère spécial ne peut être utilisé. Un mot de passe avec d'autres caractères spéciaux n'est pas autorisé.
Caractères spéciaux exclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez `@$ !`, les caractères spéciaux dans leurs mots de passe ne peuvent pas être utilisés par les utilisateurs « @ », « $ » et « ! ». **Remarque :** Cette option est disponible si la *`glide.password_policy.use_excluded_special_ch`* propriété est activée.
Interdire les données utilisateur	Option pour interdire les données utilisateur liées à l'authentification.
Seuil de longueur de séquence	La longueur de la séquence de votre mot de passe.
Seuil de longueur de répétition	La longueur de répétition de votre mot de passe. **Remarque :** ◦ Le seuil de longueur de séquence et le seuil de longueur de répétition peuvent contenir un maximum de huit caractères. Ces champs vous permettent de restreindre les combinaisons faibles de mots de passe qui ont des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$ %^ », « aaaaa », etc. ◦ Si le **préréglage de la force du mot de passe** est défini sur **Fort par défaut**, la longueur du seuil de longueur de séquence et du seuil de longueur de répétition est définie sur quatre caractères.
Testez votre mot de passe	Spécifiez votre mot de passe réel dans ce champ.

6. Cliquez sur **Tester votre mot de passe**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Une fois que la validité du mot de passe a été testée, cliquez sur **Soumettre** pour soumettre le mot de passe.

Remarque :
Testez toujours votre mot de passe avant de soumettre.

Propriétés de la politique de mot de passe

Les propriétés de la politique de mot de passe vous permettent d'administrer les politiques de mot de passe, d'exclure la liste des mots de passe et d'appliquer une politique de mot de passe pendant la connexion.

Accédez à la **Politique de mot de passe** > **Propriétés** pour afficher et modifier les propriétés de la politique de mot de passe.

Propriété	Description
glide.enable.password_policy	Active une politique de mot de passe pour votre instance. La politique entre en vigueur lorsqu'un utilisateur modifie ou réinitialise un mot de passe. Cette propriété est automatiquement définie sur **vrai**. **Remarque :** • Si votre instance est personnalisée, via la sortie d'installation ou votre `ValidatePasswordStronger` banque d'informations d'identification Réinitialisation du mot de passe [pwd_cred_store], vous devez créer cette propriété et l'ajouter à vos propriétés système. • Avant la Orlando version, si votre instance était personnalisée avec la sortie d'installation `ValidatePasswordStronger` , vous deviez créer la propriété Politique de mot de passe pour que la politique de mot de passe fonctionne. • À partir de la version, il n'y a pas de personnalisation de sortie d'installation Orlando . Les propriétés de la politique de mot de passe fonctionnent par défaut. Ces propriétés peuvent être désactivées manuellement.
glide.enable.blacklist_password	Interdit l'utilisation de mots de passe spécifiques. L'administrateur peut insérer des mots de passe dans la table Mot de passe exclu. Cette propriété est automatiquement définie sur **vrai**.
glide.apply.password_policy.on_login	Oblige les utilisateurs à changer les mots de passe lors de leur prochaine connexion si les mots de passe existants ne sont pas conformes à la politique de mot de passe actuelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Cette propriété est automatiquement définie sur **false**. Définir la valeur sur **vrai** applique une politique de mot de passe lors de la connexion. **Remarque :** L'activation de cette propriété peut forcer un nombre important d'utilisateurs qui ne sont pas en conformité avec la nouvelle politique de mot de passe à changer leur mot de passe.
glide.password_policy.user_excluded_special_char	Permet aux utilisateurs d'utiliser l'option de caractère spécial exclu sur le formulaire de politique de mot de passe.
glide.validate.sys_utilisateur.motdepasse.champ	Active la validation du mot de passe de l'utilisateur par rapport à la politique de mot de passe lorsqu'un administrateur modifie le formulaire sys_user ou la vue de liste.
glide.password.policy.generate.password.field.disabled	Désactive le champ **Mot de passe** de la fenêtre contextuelle Définir le mot de passe du formulaire sys_user.
glide.user.show.password.field	Active le champ **Mot de passe** sur le formulaire sys_user.
glide.password_policy.debug	Active la journalisation de débogage pour la politique de mot de passe.

Configurez votre politique de mot de passe

Les critères de politique de mot de passe vous permettent de sécuriser votre mot de passe et de respecter les exigences minimales de complexité des mots de passe.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le module d'extension Politique de mot de passe [com.glide.password_policy] est activé par défaut. Elle entre en vigueur lorsqu'un utilisateur modifie ou réinitialise le mot de passe. Si vous avez personnalisé votre instance, via la sortie d'installation ValidatePasswordStronger ou votre banque d'informations d'identification Réinitialisation du mot de passe [pwd_cred_store], consultez les propriétés de la politique de mot de passe.

Procédure

1. Accédez à la **Tous** > **Politique de mot de passe** > **Politiques de mot de passe**.

   Remarque :
   Préréglage fort par défaut activé par défaut Critères d'acceptation du mot de passe. Si vous souhaitez ajouter un nouveau critère, vous pouvez procéder comme suit.

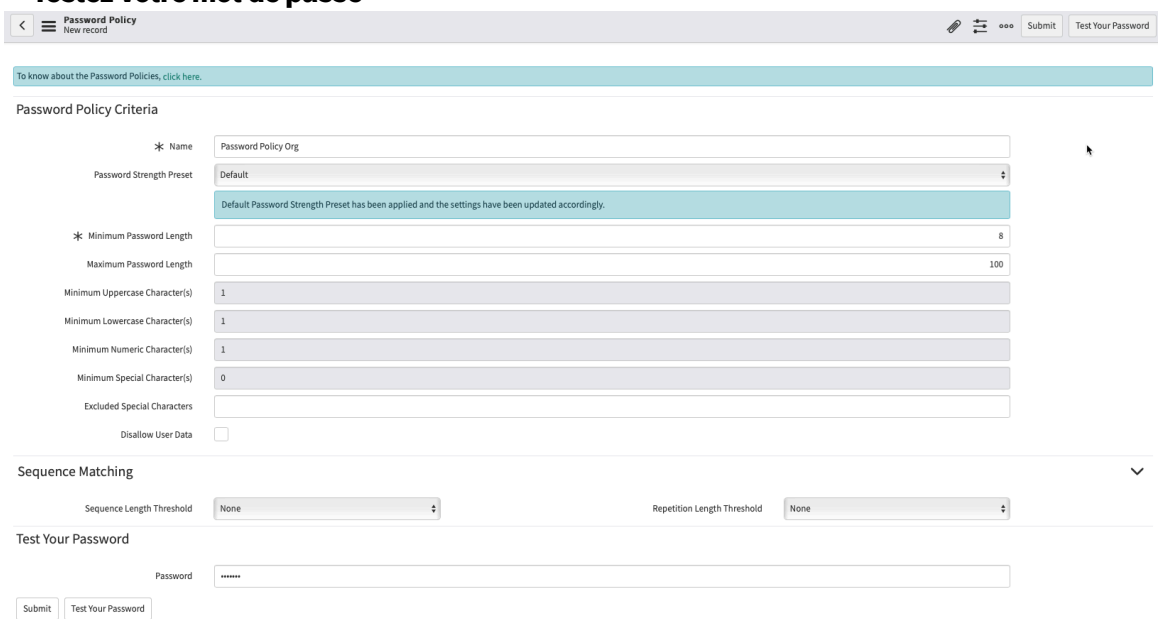
2. Cliquez sur **Nouveau**.

   La page Nouvel enregistrement de politique de mot de passe comporte les sections suivantes que vous devez spécifier pour définir votre mot de passe :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Critères de politique de mot de passe**
- **Correspondance de la séquence**
- **Testez votre mot de passe**



3. Spécifiez le **nom** de votre politique de mot de passe.
4. Dans la section **Critères de politique de mot de passe** , sélectionnez le paramètre prédéfini à partir du **Paramètre prédéfini de niveau de sécurité du mot de passe**. Les paramètres prédéfinis disponibles sont les suivants :

Force du mot de passe prédéfinie et sa description

Force du mot de passe prédéfinie	Description
Par défaut	Si vous sélectionnez **Par défaut** , les caractères de mot de passe requis sont remplis automatiquement, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum
Moyen	Si vous sélectionnez **Moyen** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum
Élevé	Si **vous sélectionnez Élevé** , les caractères de mot de passe suivants sont remplis automatiquement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Force du mot de passe prédéfinie	Description
	○ Un caractère majuscule minimum ○ Deux caractères minuscules minimum ○ Un caractère numérique minimum ○ Trois caractères spéciaux minimum
Fort par défaut	Si vous sélectionnez **Fort par défaut** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum
Personnalisé	Si **vous sélectionnez Personnalisé** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum Vous pouvez également personnaliser le **script de politique de mot de passe** qui s'affiche.
Avancés	La sélection **d'Avancé** affiche **le script de règle de mot de passe** et le **script de force du mot de passe**. En fonction de vos besoins, vous pouvez personnaliser ces scripts.

Remarque :
La politique de mot de passe est appliquée en fonction du paramètre prédéfini sélectionné.

5. Spécifiez les champs décrits dans la table :

Formulaire Politique de mot de passe

Champ	Description
Longueur minimale du mot de passe	Longueur minimale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : **Longueur minimale du mot de passe** est un champ obligatoire et il est recommandé de le définir sur un minimum de 8 à 10 caractères.
Longueur maximale du mot de passe	Longueur maximale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**. **Remarque :** **Longueur maximale du mot de passe** est un champ facultatif et il est recommandé de le définir sur un maximum de 100 caractères.
Caractère(s) majuscule(s) minimum	Nombre minimum de caractères majuscules dans le mot de passe, de 0 à 10.
Caractère(s) minuscule(s) minimum	Nombre minimum de caractères minuscules dans le mot de passe, de 0 à 10.
Caractère(s) numérique(s) minimum	Nombre minimum de caractères dans le mot de passe, de 0 à 10.
Caractère(s) spécial(ux) minimum	Nombre minimum de caractères spéciaux dans le mot de passe, de 0 à 10.
Caractères spéciaux inclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez « $, ! », les utilisateurs peuvent uniquement utiliser « $ » et « ! » comme caractères spéciaux dans le mot de passe. Aucun autre caractère spécial ne peut être utilisé et un mot de passe avec d'autres caractères spéciaux n'est pas autorisé.
Caractères spéciaux exclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, lorsque « @$! » est saisi, les caractères spéciaux que ne peuvent pas inclure les utilisateurs dans leurs mots de passe sont « @ », « $ » et « ! ». **Remarque :** Cette option est disponible si la propriété glide.password_policy.use_excluded_special_char est activée.
Interdire les données utilisateur	Cela est activé pour interdire les données utilisateur.

6. Dans la section Correspondance de la séquence, spécifiez le **seuil de longueur** de séquence et le **seuil de longueur de répétition**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le seuil de longueur de séquence et le seuil de longueur de répétition peuvent contenir un maximum de huit caractères. Ces champs vous permettent de restreindre les combinaisons faibles de mots de passe qui ont des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$ %^ », « aaaaa », etc.
- Pour **l'option Fort par défaut**, la longueur du seuil de longueur de séquence et du seuil de longueur de répétition est sélectionnée sur quatre caractères.

7. Dans la section **Tester votre mot de passe** , spécifiez votre mot de passe.
8. Cliquez sur **Tester votre mot de passe**.
9. Une fois le mot de passe valide, cliquez sur **Soumettre** pour soumettre le mot de passe.

Remarque :
Testez toujours votre mot de passe avant de soumettre.

Configurer le mot de passe d'un utilisateur

Définissez le mot de passe de votre utilisateur pour l'instance en fonction de la politique de mot de passe configurée.

Avant de commencer
Utilisateurs créés pour définir le mot de passe de leur première connexion. Pour plus d'informations, voir Créer un utilisateur .

Pour renseigner le champ **Mot de passe** directement sur le formulaire utilisateur, activez l'option **Activer pour afficher le champ Mot de passe sur le formulaire sys_user** (glide.user.show.password.field). Pour en savoir plus sur les propriétés, reportez-vous à la section Propriétés de la politique de mot de passe.

Rôle requis : admin

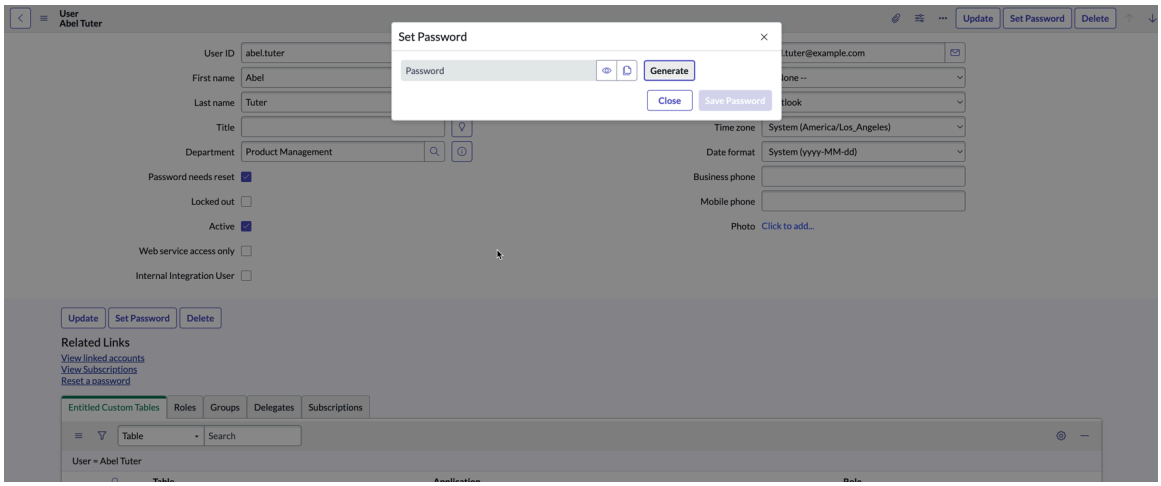
Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dans la liste de la page Utilisateurs.
3. Pour définir le mot de passe en fonction de la politique de mot de passe, cliquez sur **Définir le mot de passe**.

   La fenêtre contextuelle Définir le mot de passe s'affiche.

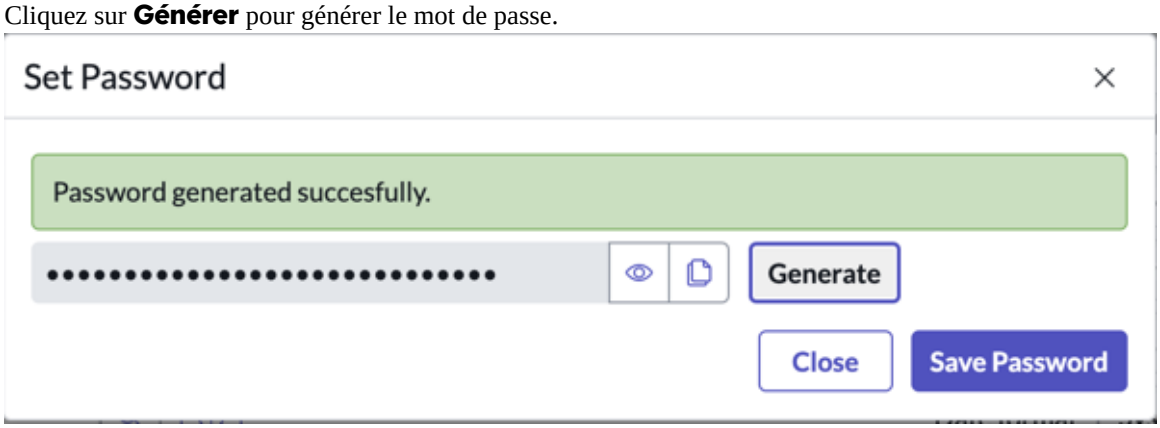
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

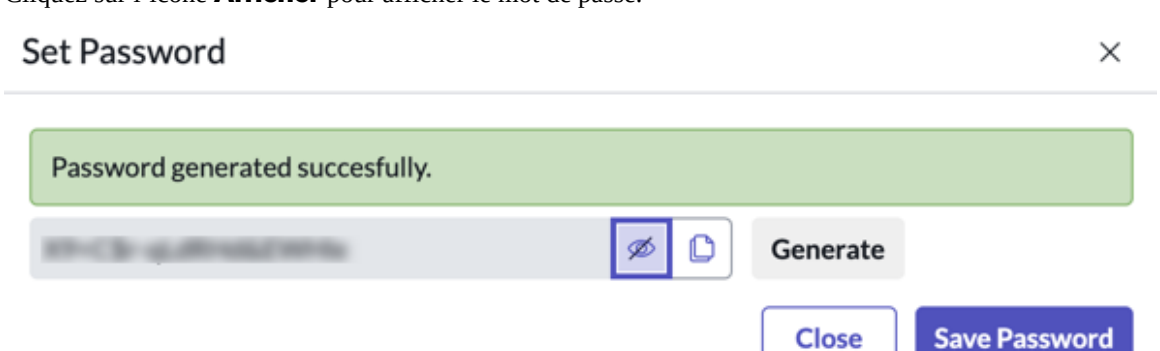


4. Dans Définir le mot de passe, procédez comme suit.

a. Cliquez sur **Générer** pour générer le mot de passe.



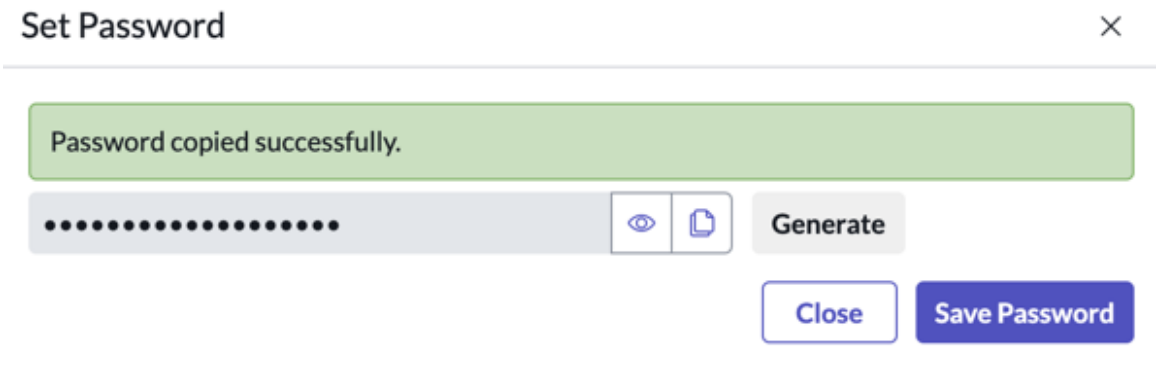
b. Cliquez sur l'icône **Afficher** pour afficher le mot de passe.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Cliquez sur l'icône **Copier** pour copier le mot de passe à partager avec l'utilisateur.



5. Cliquez sur **Enregistrer le mot de passe**.

   Le mot de passe est défini pour l'utilisateur. De plus, la case à cocher Mot de passe requiert le repos est automatiquement activée.

   Lors de la première connexion, l'utilisateur doit utiliser le même mot de passe pour la connexion et changer le mot de passe lors de la connexion en respectant la politique de mot de passe configurée par les administrateurs.

Exclure les mots de passe via les politiques de mot de passe sur votre instance

Ajoutez des mots de passe à la table Mot de passe exclu pour interdire l'utilisation de mots de passe spécifiques par les utilisateurs de votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous pouvez interdire autant de mots de passe que nécessaire. Voici quelques exemples :

- Séquences prévisibles et répétitives, telles que « 123456 », « qwerty », « !@#$ %^ », « aaaaa », etc.
- Nom de l'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que siège social d'une société, ville, pays, etc.
- Termes internes ou abréviations spécifiques à l'entreprise.
- Emojis.

Procédure

1. Accédez à la **Tous** > **Politique de mot de passe** > **Mots de passe exclus**.
2. Pour ajouter un mot de passe à votre liste d'exclusion, cliquez sur **Nouveau** et saisissez le mot de passe.
3. Accédez à la **Politique de mot de passe** > **Gestion de la liste d'exclusion** pour régir le mot de passe de vos utilisateurs et empêcher les utilisateurs d'utiliser un mot de passe incorrect pour l'instance.

   La **gestion de la liste d'exclusion** compte environ 5000 mots de passe couramment utilisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Caractères de mot de passe non pris en charge

Certains caractères de mot de passe ne sont pas pris en charge. Les utilisateurs ne peuvent pas utiliser ces caractères, en raison des exigences de ServiceNow complexité du mot de passe.

Pour activer un environnement réseau sécurisé, il est nécessaire que les utilisateurs utilisent des mots de passe forts qui incluent une combinaison de lettres, de chiffres et de symboles. Ces combinaisons aident à empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées pour deviner des mots de passe faibles.

- Les exigences de la politique en matière de mots de passe sont basées sur le plan multilingue de base (BMP) qui contient des caractères pour toutes les langues modernes. ServiceNow est livrée avec des BMP d'environ 10 000 caractères.
- Les caractères de mot de passe dans ces BMP autorisées peuvent être définis pour votre instance. Les caractères de mot de passe qui ne respectent pas ces BMP ne sont pas autorisés.

Remarque :
Les caractères spécifiques à l'utilisateur ou à la société qui ne peuvent pas être utilisés dans le mot de passe peuvent être configurés dans la liste des mots de passe d'exclusion.

Pour plus d'informations sur les propriétés de la politique de mot de passe, consultez Propriétés de la politique de mot de passe.

Réinitialisation du mot de passe

Le processus en libre-service Réinitialisation du mot de passe par défaut permet à un utilisateur de réinitialiser le mot de passe sans l'aide des agents du centre de services.

Example: Flux de réinitialisation du mot de passe en libre-service par défaut

1. Si un utilisateur ne se souvient pas du mot de passe, il peut cliquer sur le lien **Mot de passe oublié ?** sur l'écran de connexion.
2. L'application Réinitialisation du mot de passe démarre. Sur la page **Identité** , l'utilisateur s'identifie en saisissant un **nom d'utilisateur**.
3. Sur la page **Vérifier** , l'utilisateur prouve qu'il est bien la personne associée au nom d'utilisateur. Dans cet exemple, l'utilisateur saisit l'adresse e-mail associée au profil d'utilisateur. L'administrateur peut configurer une méthode de vérification différente ou peut exiger des vérifications supplémentaires, par exemple, une question personnelle à laquelle seul l'utilisateur peut répondre.
4. La page **Réinitialiser** indique à l'utilisateur de consulter les e-mails pour obtenir des instructions.
5. L'utilisateur ouvre l'e-mail et clique sur le lien **ici** pour réinitialiser le mot de passe. Le lien est valide pendant une période que vous spécifiez (utilisez la propriété**password_reset.request.expiration**).
6. La page **Réinitialiser le mot de passe** guide l'utilisateur pour réinitialiser le mot de passe.

Le processus en libre-service Réinitialisation du mot de passe par défaut (com.glideapp.password_reset) définit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'URI qui spécifie où les utilisateurs sont redirigés lorsqu'ils cliquent sur **Mot de passe oublié ?**. Par défaut, cette valeur est **/$pwd_reset.do ?sysparm_url=ss_default**, qui est la même valeur utilisée dans la `glide.security.password_reset.uri` propriété. Dans les versions précédentes, cette valeur était définie sur **/reset_password.do**.
- L'option **Activer l'URL de réinitialisation du mot de passe** , qui spécifie que l'utilisateur doit recevoir un e-mail contenant un lien pour réinitialiser son mot de passe après avoir **cliqué sur Mot de passe oublié ?**.
- Le flux de vérification Données personnelles - Entrer l'adresse e-mail qui spécifie le flux de réinitialisation du mot de passe en trois étapes.

Consultez la rubrique Configurer votre processus de réinitialisation du mot de passe pour obtenir des instructions sur l'accès à ce formulaire et la configuration des champs.

Remarque :

- Cette fonctionnalité fonctionne pour les utilisateurs authentifiés localement qui entrent le nom d'utilisateur et le mot de passe spécifiés dans leur enregistrement utilisateur. Les utilisateurs qui se connectent à l'instance via une solution SSO ou une intégration LDAP ne peuvent pas réinitialiser leur mot de passe à l'aide de l'exemple de processus en libre-service Réinitialisation du mot de passe .
- L'utilisateur final doit activer et configurer les préférences de notification. Voir Notifications basées sur un abonnement . Les administrateurs peuventx modifier l'e-mail envoyé à l'utilisateur final.

Modifier le texte de l'e-mail de Réinitialisation du mot de passe notification

Les utilisateurs du processus en libre-service Réinitialisation du mot de passe reçoivent une notification par e-mail lorsqu'ils demandent une réinitialisation du mot de passe. Vous pouvez modifier le texte de l'e-mail et d'autres aspects de la notification.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Ce processus n'est pertinent que si les utilisateurs sont des notifications basées sur un abonnement .

Procédure

1. Accédez à la **Tous** > **Notification système** > **Notifications**.
2. Sélectionnez la notification **URL de réinitialisation du mot de passe** .
3. Modifiez le texte de l'e-mail dans la section **Ce qu'il contiendra** .
   Pour plus d'informations sur la configuration d'autres aspects de la notification, voir Créer une notification par e-mail .

Configurer les Réinitialisation du mot de passe propriétés

Vous pouvez spécifier des propriétés qui configurent l'expérience des Réinitialisation du mot de passe utilisateurs finaux.

Avant de commencer

Rôle requis : password_reset_admin

Pourquoi et quand exécuter cette tâche

Bien qu'il n'y ait pas de limite de plage pour les valeurs que vous pouvez saisir pour les propriétés, envisagez d'utiliser uniquement des valeurs entières positives commençant par

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Lorsque vous déterminez la limite de la plage supérieure d'une propriété, tenez compte de la tâche que l'utilisateur effectue.

Par exemple, vous ne voudriez pas autoriser 100 tentatives pour que les utilisateurs vérifient leur identité. Une valeur plus courante est de 3 tentatives. De même, vous ne voudrez peut-être pas forcer les utilisateurs qui terminent le processus d'inscription à passer du temps à sélectionner et à répondre à 30 questions de sécurité. Le nombre de questions de sécurité le plus couramment utilisé se situe entre 5 et 7.

Procédure

1. Accédez à la **Tous** > **Réinitialisation du mot de passe** > **Propriétés**.
   Pour en savoir plus sur les Réinitialisation du mot de passe propriétés, reportez-vous à la rubrique Réinitialisation du mot de passe Propriétés globales .
2. Mettez à jour les paramètres selon vos besoins, puis cliquez sur **Enregistrer**.

Mémoriser mon nom

Lorsque la case **Se souvenir de moi** est cochée lors de la connexion, un cookie est stocké sur l'ordinateur de l'utilisateur. Ce cookie authentifie automatiquement l'utilisateur lors des visites ultérieures.

Si l'utilisateur se déconnecte, le cookie est détruit. La valeur par défaut de la case à cocher **Se souvenir de moi** est contrôlée par une propriété, et l'affichage ou non de la case à cocher sur la page de connexion est contrôlé par une autre propriété.

Deux propriétés `glide.ui.user_cookie.life_span_in_days` et `glide.ui.user_cookie.max_life_span_in_days` contrôlent la valeur d'expiration de cookie générée par le système glide_user. Lorsqu'un utilisateur accède à une instance avec l'option « Se souvenir de moi » activée, l'accès réinitialise la période d'expiration du cookie jusqu'à ce que la limite maximale de la durée de vie (glide.ui.user_cookie.max_life_span_in_days) soit atteinte.

Remarque :
Pour en savoir plus sur ces propriétés, consultez les rubriques suivantes dans Paramètres de renforcement de la sécurité de l'instance :

- Minimiser la durée du délai absolu d'expiration de la session [Mis à jour dans Centre de sécurité 1.3]
- Minimiser la durée du délai d'expiration de la fenêtre de session [Mis à jour dans Centre de sécurité 1.3]

Modifier la valeur par défaut de la case à cocher Se souvenir de moi

Vous pouvez modifier la valeur par défaut de la case à cocher **Se souvenir de moi** .

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Propriétés de l'interface utilisateur**.
2. Localisez la `Default value of "Remember me" checkbox on login page` propriété (`glide.ui.remember.me.default`).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Pour définir la valeur par défaut de la case à cocher **Se souvenir de moi** sur **Non**, décochez la case de propriété.
4. Pour restaurer la valeur par défaut de la case à cocher **Se souvenir de moi** sur **Oui**, cochez la case de propriété.

Supprimer la case à cocher Se souvenir de moi

Vous pouvez décocher la case **Mémoriser** mon nom pour que les utilisateurs n'aient pas accès à cette fonctionnalité.

Avant de commencer
Rôle requis : security_admin

Remarque :
Pour en savoir plus sur cette propriété, consultez Supprimer Se souvenir de moi Paramètres de renforcement de la sécurité de l'instance.

Procédure

1. Élevez votre rôle à security_admin.
2. Accédez à la **Propriétés système** > **Propriétés de l'interface utilisateur**.
3. Localisez la *`Remove "Remember me" checkbox from login page`* propriété (*`glide.ui.forgetme`*).
4. Cochez la case de la propriété.
   Ce paramètre supprime la case à cocher **Se souvenir de moi** , invalide les cookies existants et désactive entièrement la fonctionnalité Se souvenir de moi.
5. Pour restaurer la case à cocher **Se souvenir de moi** sur la page de connexion, décochez la case de propriété.

Configurer l'invite de confirmation de déconnexion

Vous pouvez activer une invite de confirmation de déconnexion pour empêcher les utilisateurs de se déconnecter par inadvertance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :
La procédure suivante ne fonctionne que dans les versions d'interface utilisateur antérieures à Interface utilisateur principale, qui est la plus récente et la plus couramment utilisée.

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Système**.
2. Localisez la propriété **Inviter l'utilisateur à confirmer une demande de déconnexion** et cochez la case.
3. Lorsque l'utilisateur clique sur le bouton **Déconnexion** , une boîte de dialogue de confirmation s'affiche.

Implémenter une valeur de circonstance

Vous pouvez implémenter une valeur de circonstance à utiliser avec l'authentification synthèse d'authentification unique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour utiliser une valeur de circonstance avec les méthodes de jeton non chiffré ou de jeton chiffré de l'authentification unique, ces étapes s'appliquent avec seulement quelques modifications mineures.

Remarque :
La valeur de circonstance n'est utilisée que pour les demandes de connexion, pas pour tout autre type de demande. Si le système reçoit une valeur de valeur de valeur de circonstance après la connexion, celle-ci n'est pas consommée.

Avantages

L'utilisation d'une valeur de circonstance empêche un utilisateur malveillant d'effectuer une attaque par relecture afin de se connecter à votre système.

Flux de processus de nonce

Lorsqu'un client a implémenté le jeton digéré Single Sign-on et souhaite ajouter la sécurité d'un nonce, il suit un certain flux de processus.

1. Un utilisateur se connecte au portail du client.
2. Le client génère les paramètres SSO requis et ajoute une valeur de circonstance aléatoire à la fin. Par exemple, si le client transmettait la réponse d'authentification via la chaîne de requête, elle pourrait ressembler à ceci :

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

L'instance reçoit cette demande et récupère les variables d'authentification. Avant d'essayer de vérifier l'intégrité de la réponse d'authentification, l'instance vérifie la valeur de circonstance par rapport à une table interne (u_authentication_nonce) pour vérifier qu'elle n'existe pas encore. Si la valeur de circonstance n'existe pas dans cette table, elle est ajoutée à la table et le processus d'authentification peut se poursuivre. Toutefois, si cette valeur de valeur de circonstance existe déjà dans la table, la tentative d'authentification est annulée et un code d'erreur de `failed_missing_requirement` est renvoyé, ce qui renvoie généralement l'utilisateur à la page de connexion.

Implémenter une valeur de circonstance

Ajoutez une valeur de circonstance cryptographique à l'en-tête d'authentification pour vous assurer qu'elle ne peut être utilisée qu'une seule fois.

- Créez une propriété système appelée *`glide.authenticate.header.nonce_key`* et définissez sa valeur sur le nom de variable que vous utilisez pour le nonce, tel que NONCE ou NCE.
- Créez une table appelée `u_authentication_nonce`. Ajoutez un champ à la table appelé `u_nonce`.
- Accéder à **Propriétés système** > **Sorties d'installation** et créez un élément appelé DigestSingleSignOnNonce qui remplace ExternalAuthentication (*`glide.authenticate.external_property`*).
- Ajoutez le code suivant à la partie script du DigestSingleSignOnNonce nouvellement créé.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
process : function() {

 var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
 var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key",
"DIGEST");
 var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
 var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
 var fkey = GlideProperties.get("glide.authenticate.secret_key");

 // Look in the Headers
 var data = request.getHeader(headerKey);
 var encdata = request.getHeader(headerDigestKey);
 var nonce = request.getHeader(headerNonceKey);

 // If not, then check the URL Parameters
 if (data == null || encdata == null || nonce == null) {
  data = request.getParameter(headerKey);
  encdata = request.getParameter(headerDigestKey);
  nonce = request.getParameter(headerNonceKey);
 }

 // then maybe its a cookie
 if (data == null || encdata == null || nonce == null) {
  var cookies = request.getCookies();
  data = GlideCookieMan.getCookieValue(cookies, headerKey);
  encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
  nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
 }

 // if found run encryption
 if (data != null && encdata != null && nonce != null) {
  try {

   // Replace all spaces with plus(+)'s, converted in url
   encdata = encdata.replaceAll(' ', '+');

   // ----- Encrypt the username|nonce
   var key = this.getDigest( data + "|" + nonce, fkey);

   // Check for match of received encoded data
   // and your encoding of user name
   if (encdata == key) {
    var ugr = new GlideRecord("sys_user");
    ugr.initialize();
    if (!ugr.isValidField(fieldName)) {
     GlideLog.warn("External authorization is set to use field: '"+ fieldName + "' which doesn't
exist");
     return "failed_missing_requirement";
    }
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next()) {
     var userLoad = GlideUser.getUser(data);
     if (userLoad == null)
      return "failed_authentication";

     ugr.initialize();
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next())
     return "failed_authentication";

   }

   if (this.processNonce(nonce)){
    var userName = ugr.getValue("user_name");
    return userName;
   }
   else return "failed_missing_requirement";
   }
  else {

   return "failed_authentication";
  }
 } catch(e) {
  gs.log(e);
  return "failed_authentication";
 }
 // Encoded data didn't match recieved Encoded data
} else {

 return "failed_missing_requirement";
}
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
};
```

- Une fois que vous avez enregistré votre nouvelle sortie d'installation, accédez à la sortie d'installation DigestSingleSignOn et assurez-vous qu'elle est définie sur Active=false.

Votre instance doit maintenant être configurée pour implémenter un nonce.

Authentification multifacteur

Découvrez comment activer, utiliser et configurer l'authentification multifacteur (MFA).

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l'authentification multifacteur.

Configurer



Découvrez comment activer l'authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser



Utilisez la MFA.

MFA avec authentification unique (SSO)



Découvrez comment configurer la MFA avec authentification unique (SSO).

Application de l’authentification multifacteur

Application de la MFA pour les connexions non SSO à ServiceNow partir de la version Yokohama.

La MFA renforce la sécurité en exigeant des utilisateurs qu’ils fournissent deux preuves ou plus pour prouver leur identité lors de la connexion. L’authentification multifacteur protège les comptes contre les menaces telles que l’hameçonnage et les prises de contrôle de comptes.

La MFA étant un outil de sécurité essentiel contre diverses attaques liées à la prise de contrôle d’identité. ServiceNow applique la MFA par défaut après la mise à niveau de Yokohama et la rend obligatoire pour les connexions non SSO (utilisateurs effectuant une connexion avec uniquement un nom d’utilisateur et un mot de passe ou une authentification basée sur LDAP) afin d’assurer une meilleure posture de sécurité et de réduire le risque de violations.

L’application de la MFA s’effectue par le biais d’une stratégie MFA qui est activée par défaut à partir de Yokohama ou mise à niveau vers Yokohama.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- La politique est activée pour tous les utilisateurs **non snc_external** effectuant une authentification locale (nom d'utilisateur et mot de passe) ou basée sur LDAP.
- L'administrateur de l'instance peut modifier le périmètre de l'application en changeant la politique de contexte MFA, les critères de politique ou les conditions de politique.

Voici plus de détails sur l'application de la MFA :

- Appliqué à toutes les instances de production et de non-production.
- Appliqué à tous les utilisateurs **non snc_external** et à la connexion **non SSO** .
- L'intégration avec l'authentification de base et l'attribution des informations d'identification du mot de passe du propriétaire de ressource OAuth ne nécessite pas l'authentification MFA de Yokohama.

Pour en savoir plus sur les changements dus à l'application, reportez-vous à la section Changements dus à l'application de l'authentification multifacteur.

Pour en savoir plus sur l'authentification multifacteur, reportez-vous à la section Explorer l'authentification multifacteur.

Information associée

Configuration de l'authentification multifacteur

Utilisation de l'authentification multifacteur

Propriétés de l'application de l'authentification multifacteur

Dépannage de l'application de l'authentification multifacteur

Forum Aux Questions - Application de l'authentification multifacteur

Changements dus à l'application de l'authentification multifacteur

Informations sur les changements attendus en raison de l'application de la MFA.

Changements d'application de la MFA attendus comme suit :

- Aucun impact sur l'intégration.
- Les utilisateurs qui ont déjà souscrit à la MFA continuent d'être confrontés à la MFA lors de la connexion locale.
- Si un utilisateur n'a pas encore configuré l'authentification multifacteur après la mise à niveau de Yokohama, il sera initialement exempté de l'authentification multifacteur pendant une certaine période au cours de laquelle il pourra s'inscrire à l'authentification multifacteur.
- Si l'utilisateur ne parvient pas à s'inscrire lui-même, il voit l'authentification multifacteur appliqué à l'issue de la période d'exemption (30 jours par défaut) et doit configurer l'authentification multifacteur.
- Après 90 jours, la MFA sera appliquée par défaut. Il n'y aura pas de période d'auto-inscription pour les premières connexions après 90 ans. Les administrateurs peuvent configurer cette période.

En tant qu'administrateur, vous pouvez vous préparer à l'application de la MFA en fonction des éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Passez en revue la configuration de la politique de contexte MFA et ajustez les conditions de la politique en fonction des besoins de votre entreprise.
- Ajoutez le groupe exempté fourni par défaut, s'il existe d'autres utilisateurs qui doivent être exemptés.
- Passez en revue les propriétés d'application de la MFA et ajustez-les en fonction de vos besoins. Pour en savoir plus, consultez Propriétés de l'application de l'authentification multifacteur.

Example: Scénario d'application de la MFA après 30 jours d'application de la MFA

- **Scénario 1 pour ACME Corp** : dans l'instance, si l'utilisateur n'a pas de politique MFA active. Imagine Sarah utilise l'authentification locale pour accéder à une instance. Lors de la mise à niveau vers la version Yokohama pendant la connexion, un message d'inscription à la MFA s'affiche. Vous avez 30 jours pour terminer cette configuration. Si Sarah ne termine pas la configuration, après 30 jours, le compte nécessite une connexion MFA et ne pourra pas y accéder tant que la MFA n'est pas configurée.
- **Scénario 2 pour Acme Corp** : dans l'instance, Anita était déjà MFA avec l'authentification locale. Anita continue d'exiger une MFA sans la fenêtre d'auto-inscription de 30 jours.
- **Scénario 3 pour ACME Corp** : dans l'instance, Olivia utilise l'authentification unique (SSO) pour l'authentification. Il n'y a aucun impact sur l'expérience de connexion et Olivia n'est pas appliqué pour la MFA.
- **Scénario 4 pour Globex Corp** : Dans le cas, si un utilisateur avait déjà une politique MFA exigeant une MFA pour toutes les tentatives de connexion locale en dehors du réseau de confiance de l'entreprise. Lors de la mise à niveau vers Yokohama ou une version ultérieure, le comportement d'application de la MFA pour les connexions utilisateur reste le même.

Propriétés de l'application de l'authentification multifacteur

Configurez les propriétés pour l'application de la MFA à partir de Yokohama et effectuez une mise à niveau vers Yokohama.

Pour définir les propriétés d'application de la MFA, accédez à **sys_properties.list** pour valider ou modifier les propriétés d'application de la MFA.

Propriétés d'application de la MFA

Champ	Description
`glide.authenticate.multifactor.setup.bypass.count`	Nombre de fois qu'un utilisateur peut contourner la configuration de l'authentification multifacteur (le nombre maximal de contournements possibles est de 3, au-delà de cela, il est traité comme 3).
`glide.authenticate.multifactor.self_enrollment_period`	Indique le nombre de jours pendant lesquels un utilisateur aura la possibilité de s'inscrire automatiquement à la MFA, après quoi l'utilisateur sera automatiquement mis à l'épreuve avec la MFA. Toute valeur supérieure à 90 est traitée comme 90 jours uniquement.
`glide.authenticate.multifactor.enforcement_max_allowable_period`	Indique le nombre maximal de jours pendant lesquels un nouvel utilisateur aura la possibilité de s'inscrire automatiquement à la MFA, après quoi toutes les connexions non SSO d'un nouvel utilisateur seront

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés d'application de la MFA (suite)

Champ	Description
	automatiquement mises à l'épreuve avec la MFA. Toute valeur supérieure à 270 est traitée comme 270 jours uniquement.
glide.authenticate.multifactor.enforcement.debug	Enregistrement de débogage de l'application MFA. Permet de déboguer les flux pour les connexions MFA. **Remarque :** Cette propriété n'existe pas sur l'instance. Vous devez créer et activer la propriété, si nécessaire.
glide.authenticate.hybrid_user_tracking.enabled	Propriété pour le suivi des utilisateurs hybrides. Les comptes d'utilisateurs qui ne sont pas marqués comme « Accès au service Web uniquement » dans l'enregistrement de sys_user correspondant, mais qui effectuent quand même des intégrations (par exemple, des connexions API) à l'aide du nom d'utilisateur et du mot de passe, sont suivis dans la table « Informations de connexion de l'utilisateur » lorsque cette propriété est activée. **Remarque :** Cette propriété n'existe pas sur l'instance. Vous devez créer et activer la propriété, si nécessaire.
glide.authenticate.hybrid_user_tracking.debug	Un enregistreur de débogage pour le suivi des connexions d'API d'utilisateurs hybrides. Côté **Remarque :** Cette propriété n'existe pas sur l'instance. Vous devez créer et activer la propriété, si nécessaire.

Dépannage de l'application de l'authentification multifacteur

Informations de dépannage dues à l'application de la MFA.

ServiceNow applique la MFA par défaut après la mise à niveau de Yokohama et la rend obligatoire pour les connexions non SSO (utilisateurs effectuant une connexion avec uniquement un nom d'utilisateur et un mot de passe ou une authentification basée sur LDAP) afin d'assurer une meilleure posture de sécurité et de réduire le risque de violations.

L'application de la MFA s'effectue par le biais d'une stratégie MFA qui est activée par défaut à partir de Yokohama ou mise à niveau vers Yokohama. Voici quelques-unes des tâches de dépannage que vous pouvez effectuer en cas de changement du comportement MFA :

- Déboguer à l'aide des outils de dépannage
- Accédez à l'emplacement du journal et aux propriétés de débogage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Comprendre les scénarios MFA en fonction de l'expérience de vos utilisateurs lors de l'utilisation de la MFA
- Comprendre le problème MFA dû à la mise à niveau à partir d'une version précédente

Déboguer la MFA

Utilisez l'un des outils suivants ou une combinaison des outils pour comprendre les informations de débogage :

- **Splunk** : pour afficher les journaux de débogage.
- Journaux système ou journaux de nœud.
- **Journaux HAR** pour analyser les journaux de débogage pour la MFA.

Consigner l'emplacement et les propriétés de débogage

Accédez à l'emplacement suivant pour en savoir plus sur les journaux :

- Pour les journaux système, accédez à **Tous** > **Journal système** > **Journaux système**.
- Pour les journaux de nœud, accédez à **Tous** > **Journaux système** > **Utilités** > **Navigateur de fichier journal de nœud**.

Les journaux de débogage système et les journaux de nœud d'instance sont requis à des fins de débogage. Les propriétés de débogage suivantes doivent être activées :

- `glide.webauthn.debug.enabled`
- `glide.log.default_log_debug`
- `glide.authenticate.policy.debug`
- `glide.authenticate.hybrid_user_tracking.debug`

Problème MFA basé sur des scénarios

Scénario 1 : l'utilisateur ne peut pas se connecter à l'aide de l'un de ses deuxième facteur

Réinitialisez l'authentification multifacteur pour vos utilisateurs et supprimez les anciens enregistrements utilisateur des tables suivantes :

- `user_multifactor_auth`
- `sys_user_public_credential`
- `sys_user_multi_factor_setup`

Scénario 2 : l'administrateur n'est pas en mesure de se connecter à l'aide de l'un de ses deuxième facteur

Un autre utilisateur disposant d'un accès administrateur peut réinitialiser la MFA pour n'importe quel utilisateur administrateur bloqué. Si le problème persiste, contactez le ServiceNow support.

Scénario 3 : erreur observée lors de la configuration ou de la validation de la MFA

Vérifiez l'avertissement « Codes d'erreur associés/Avertissement : votre code de vérification à 6 chiffres est incorrect. Essayez à nouveau avec le bon code".

Procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans le cas de l'application d'authentification TOTP, si la date et l'heure de l'appareil et de l'instance MFA de l'authentificateur ne sont pas synchronisées (±30 secondes), le code TOTP n'est pas accepté. Vérifiez l'appareil et la date et l'heure de l'instance.
- Dans le cas d'un e-mail, configurez correctement la notification au niveau de l'utilisateur, la configuration des e-mails sortants et l'utilisateur dans la table `sys_user` .
- En cas de SMS, configurez correctement l'intégration de Twillio ou d'un autre fournisseur de service SMS et définissez-la sur actif. Vérifiez si le numéro de téléphone portable de l'utilisateur est correctement configuré dans la table `sys_user` .

Forum Aux Questions - Application de l'authentification multifacteur

Détails sur certaines des FAQ dues à l'application de la MFA.

La MFA étant un outil de sécurité essentiel contre diverses attaques liées à la prise de contrôle d'identité. ServiceNow applique la MFA par défaut après la mise à niveau de Yokohama et la rend obligatoire pour les connexions non SSO (utilisateurs effectuant une connexion avec uniquement le nom d'utilisateur et le mot de passe ou une authentification basée sur LDAP).

L'application de la MFA s'effectue par le biais d'une stratégie MFA qui est activée par défaut à partir de Yokohama ou mise à niveau vers Yokohama. Vous pouvez consulter les liens suivants pour en savoir plus sur les questions liées à l'application de la MFA :

- Exception d'application de la MFA
- Exigences d'application de la MFA – Quoi et pourquoi
- Périmètre de l'application de la MFA
- Chronologie d'application de la MFA
- Mesures MFA
- Types de MFA
- Réinitialisation MFA

Exigences d'application de la MFA – Quoi et pourquoi

FAQ relative à l'application de la MFA et pourquoi c'est important.

1. Qu'est-ce que la MFA ?

L'authentification multifacteur (MFA) est un processus de sécurité qui vous oblige à fournir deux formes de vérification ou plus avant qu'ils puissent accéder à un compte ou à un système. Pour en savoir plus, consultez Explorer l'authentification multifacteur.

2. Pourquoi l'application de la MFA est-elle obligatoire ?

La MFA est mandatée pour protéger votre compte et la sécurité de vos données. Les cybermenaces sont en constante évolution et les mots de passe seuls ne suffisent plus à protéger contre les accès non autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsque la MFA est activée, même si les attaquants ont votre mot de passe, les attaquants ont toujours besoin d'une deuxième forme de vérification. Cette couche supplémentaire bloque considérablement la plupart des tentatives non autorisées, ce qui renforce la sécurité de vos informations.
- En définissant la MFA par défaut, minimisez le risque de failles de sécurité et protégez automatiquement votre compte. Cela signifie que vous bénéficiez d'une plus grande tranquillité d'esprit sans avoir à prendre de décisions de sécurité supplémentaires.

3. Pourquoi est-il important d'activer l'authentification multifacteur ?

L'activation de la MFA renforce la sécurité de votre compte. Les mots de passe seuls ne suffisent pas, car ils peuvent être exposés lors de violations de données. Avec l'authentification multifacteur, même si quelqu'un connaît votre mot de passe, il ne peut pas accéder à votre compte sans une deuxième étape de vérification.

4. Pourquoi l'authentification multifacteur est-elle ServiceNow nécessaire ?

ServiceNow rend obligatoire l'authentification multifacteur pour vous protéger contre ces menaces. C'est un moyen simple mais efficace de réduire les accès non autorisés. En exigeant l'authentification multifacteur, chaque compte bénéficie d'une solide couche de protection, ce qui réduit les risques de sécurité pour vous et tous les utilisateurs.

5. Quelle est l'exigence MFA pour les clients existants ?

Pour les clients existants qui mettent à niveau leur instance vers Yokohama ou une version ultérieure :

- Si **l'authentification adaptative** n'est pas déjà activée sur Contexte d'authentification multifacteur l'instance, elle est automatiquement activée en tant que politique MFA par défaut.
- Tous les utilisateurs internes (utilisateurs qui n'ont pas snc_external rôle) qui se connectent avec une authentification locale ou LDAP doivent configurer l'authentification MFA dans les 30 jours suivant leur première connexion réussie. Pendant ce temps, vous pouvez vous connecter normalement, mais un message s'affiche au moment de la connexion pour vous inscrire à l'authentification multifacteur.
- Après 30 jours, l'authentification multifacteur sera requise par défaut et les utilisateurs ne pourront pas se connecter sans avoir terminé la configuration de l'authentification multifacteur.

6. Quelle est l'exigence MFA pour les nouveaux clients ?

Pour toute instance utilisant la version Yokohama ou une version ultérieure, la MFA est activée par défaut pour tous les utilisateurs internes. Cela s'applique également aux utilisateurs qui n'ont pas le rôle snc_external et qui se connectent avec une authentification locale ou LDAP. Dès la première connexion, les utilisateurs doivent configurer et utiliser la MFA.

Périmètre de l'application de la MFA

FAQ relative au champ d'application de la MFA et à son importance.

1. Quels types d'utilisateurs, de connexions et d'environnements nécessitent l'authentification multifacteur ?

À partir de la version Yokohama, avec la nouvelle politique MFA sécurisée par défaut MFA appliquée pour les scénarios suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Tous les utilisateurs, à l'exception des utilisateurs disposant **snc_external** rôle.
- Tous les utilisateurs effectuant une authentification locale basée sur nom d'utilisateur et mot de passe ou LDAP (Lightweight Directory Access Protocol).
- Toutes les instances client, y compris les instances de production, de sous-production et de test, qui n'avaient pas déjà de politique MFA active avant la mise à niveau.

L'administrateur de l'instance peut modifier le périmètre de l'application en changeant la politique de contexte MFA, les critères de politique ou les conditions de politique.

2. La MFA est-elle requise pour les connexions SSO (Single-Sign-On) ?

Non. Avec la politique MFA sécurisée par défaut, la MFA n'est pas requise pour la connexion SSO (SAML, OIDC, authentification basée sur certificat).

Les clients peuvent collaborer avec leur fournisseur Single Sign-On (SSO) (fournisseur d'identité ou IdP) pour appliquer l'authentification multifacteur (MFA) côté IdP. S'il n'est pas possible d'appliquer la MFA du côté de l'IdP, les clients ont également la possibilité d'activer la MFA de la plateforme pour les ServiceNow connexions SSO en suivant les instructions fournies dans Authentification multifacteur avec authentification unique.

3. La MFA est-elle requise pour les utilisateurs externes ?

Non. Avec la politique MFA sécurisée par défaut, la MFA n'est pas requise pour les utilisateurs disposant du rôle snc_external.

- Les administrateurs peuvent modifier ce comportement et appliquer la MFA pour les utilisateurs externes en mettant à jour les conditions de politique de MFA.
- Les utilisateurs externes qui suivaient déjà l'authentification multifacteur avant la mise à niveau vers Yokohama ou une version ultérieure continuent d'avoir l'authentification multifacteur.
- Les utilisateurs externes peuvent visiter leur profil et s'inscrire automatiquement à la MFA.

4. La MFA est-elle requise pour la connexion à l'application mobile ?

Oui. La politique MFA est appliquée aux connexions Web et aux applications mobiles avec une connexion non SSO basée sur le nom d'utilisateur et le mot de passe.

5. La MFA est-elle requise pour les environnements de non-production et de test ?

Oui. La MFA est appliquée pour toutes les instances client, y compris les environnements de production, de non-production, de développement et de test, si aucune politique MFA active n'existait sur l'instance avant la mise à niveau vers Yokohama ou des versions ultérieures.

6. La MFA est-elle requise pour les instances de développeur ?

Oui. La MFA est appliquée pour toutes les instances de développeur qui se trouvent sur Yokohama ou des versions ultérieures.

7. La MFA est-elle requise pour l'authentification API ?

Non. À partir de Yokohama ou d'une version ultérieure, la MFA n'est requise que pour les connexions interactives des utilisateurs basés sur le nom d'utilisateur et le mot de passe. Cela signifie que l'authentification API avec authentification de base fonctionne sans nécessiter de MFA. Il est recommandé aux clients d'utiliser d'autres méthodes d'authentification d'API sécurisées telles que OAuth ou mTLS. Plus de détails ici.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Clone

b. Récupération de l'ensemble de mises à jour

c. RPA

8. La MFA a-t-elle un impact sur le processus de configuration du clone ?

   Non, le processus de configuration du clone continue de fonctionner avec le nom d'utilisateur et le mot de passe et ne nécessite pas de MFA.

9. Y a-t-il un impact sur la récupération de l'ensemble de mises à jour dû à la MFA ?

   Non, la récupération de l'ensemble de mises à jour continue de fonctionner avec le nom d'utilisateur et le mot de passe et ne nécessite pas de MFA.

10. Y a-t-il eu un impact sur l'accès des bots RPA aux ServiceNow instances ?

    Oui, si le bot RPA utilise le nom d'utilisateur interactif et le mot de passe de connexion pour accéder à l'instance, il doit effectuer une ServiceNow MFA. Les administrateurs peuvent ajouter des comptes de bot RPA au **groupe d'utilisateurs exemptés de MFA** s'ils souhaitent assouplir la MFA pour les comptes de bot RPA.

11. La MFA est-elle requise pour les intégrations basées sur OAuth ?

    Les informations d'identification du mot de passe du propriétaire de ressource OAuth (ROPC) fonctionnent avec le nom d'utilisateur et le mot de passe sans nécessiter de MFA. Pour le type d'attribution de code d'autorisation, la MFA est requise dans le cadre du flux de connexion de l'utilisateur avant de donner son consentement OAuth.

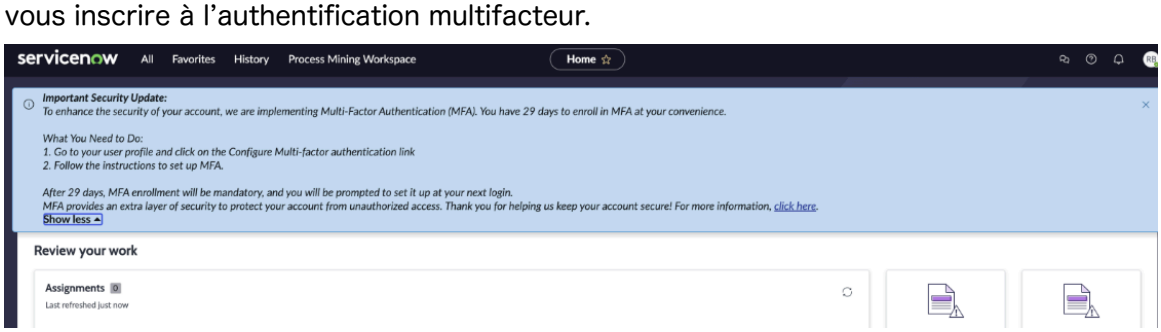
Chronologie d'application de la MFA

FAQ relative aux délais d'application de la MFA et pourquoi c'est important.

1. Quand la MFA est-elle appliquée ?

   Selon la politique MFA, les utilisateurs éligibles qui n'ont pas terminé la configuration MFA disposent d'une période d'auto-inscription de 30 jours. Le comportement est contrôlé à l'aide de la propriété système `glide.authenticate.multifactor.self_enrolment_period`. La valeur par défaut de la propriété est 30 jours. Elle peut être mise à jour jusqu'à un maximum de 90 jours.

   Tous les utilisateurs internes (utilisateurs qui ne disposent pas d'un rôle `snc_external`) qui se connectent avec l'authentification locale ou LDAP doivent configurer l'authentification MFA dans les 30 jours suivant leur première connexion. Pendant ce temps, vous pouvez vous connecter normalement, mais un message s'affiche au moment de la connexion pour vous inscrire à l'authentification multifacteur.



Après 90 jours de mise à niveau vers Yokohama ou une version ultérieure, si un utilisateur interne (utilisateur sans le rôle `snc_external`) se connecte avec une authentification locale

Traduction automatique

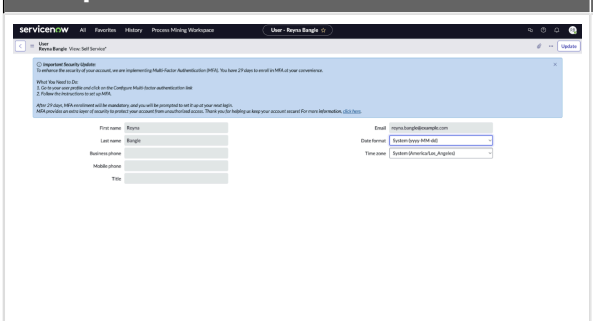
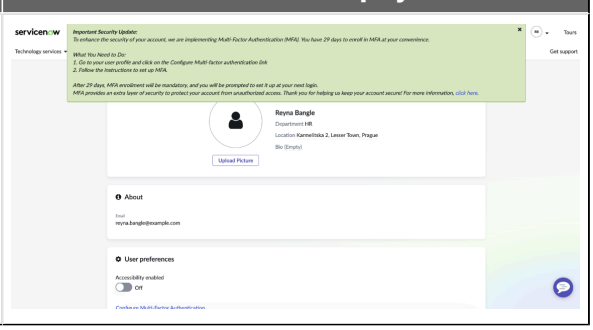
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ou LDAP pour la première fois, il devra utiliser la MFA immédiatement. Vous ne disposez pas de la fenêtre d'auto-inscription MFA de 30 jours. Cette période est régie par une propriété système : glide.authenticate.multifactor.enforcement.max_relaxation_period. La valeur maximale pour cette propriété est de 270 jours.

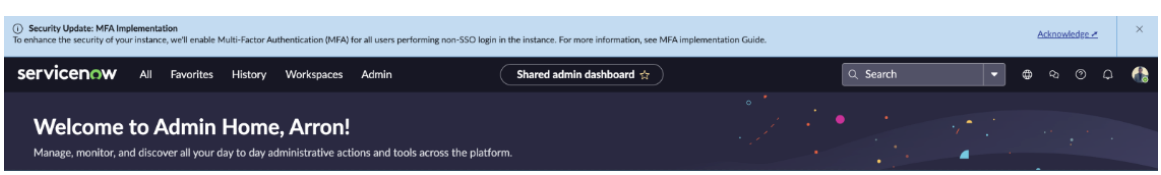
2. Comment le calendrier d'application de la MFA peut-il être ajusté ?
   - En mettant à jour la valeur du glide.authenticate.multifactor.self_enrolment_period de propriété, les administrateurs peuvent fournir une fenêtre d'auto-inscription plus petite ou plus grande. Définissez la valeur de la propriété sur 0. Les utilisateurs doivent terminer la configuration MFA après leur première tentative de connexion avec une connexion locale ou LDAP après la mise à niveau vers Yokohama ou une version ultérieure. La durée maximale de la fenêtre d'auto-inscription peut être de 90 jours. La valeur de propriété définie au-dessus de 90 sera traitée comme 90.
   - En mettant à jour la valeur de la propriété glide.authenticate.multifactor.enforcement.max_relaxation_period , l'administrateur peut décider combien de jours après la mise à niveau vers Yokohama ou une version ultérieure vous obtenez la fenêtre d'auto-inscription MFA.
3. Comment les utilisateurs finaux sont-ils informés de ce changement à venir ?

   Les utilisateurs finaux effectuant une authentification locale ou LDAP qui seront appliquées avec la MFA verront un message d'information après s'être connectés. Le même message est disponible lorsque les utilisateurs visitent leur profil.

Message d'application

Sur le profil d'utilisateur	Sur Centre de services aux employés
	

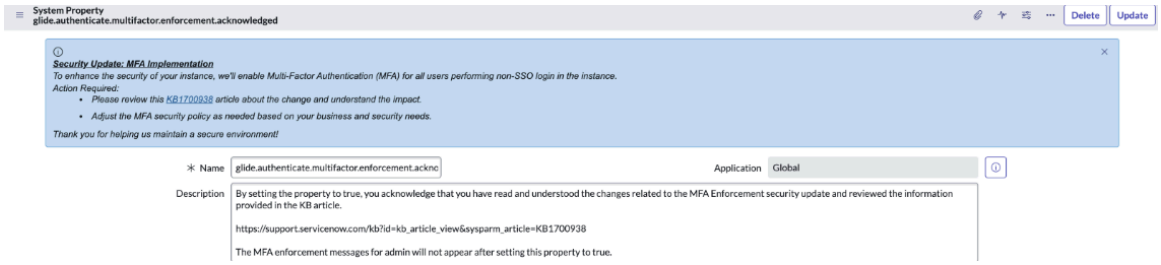
Ce message ne s'affichera pas pour les utilisateurs non-administrateurs effectuant des connexions SSO. Le rôle administrateur verra un message d'information différent après une connexion réussie, quelle que soit la méthode d'authentification utilisée pour se connecter.



Ce message continue de s'afficher jusqu'à ce que l'un des administrateurs confirme la mise à jour en définissant la valeur de la propriété glide.authenticate.multifactor.enforcement.recognized sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Comment désactiver le message affiché aux utilisateurs finaux sur l'achèvement de la configuration de la MFA lorsqu'ils se connectent ?

   Les administrateurs peuvent mettre à jour la valeur de la propriété système glide.authenticate.multifactor.enforcement.show_user_info_message sur false pour désactiver le message d'informations d'inscription à la MFA affiché aux utilisateurs finaux après la connexion.

5. Comment désactiver le message affiché aux administrateurs au sujet de l'application de la MFA ?

   Le message d'information concernant l'application de la MFA affiché aux utilisateurs administrateurs après la connexion cesse de s'afficher lorsque l'un des administrateurs le confirme en mettant à jour la valeur de la propriété système glide.authenticate.multifactor.enforcement.recognized sur vrai.

6. Il existe déjà une politique MFA définie à l'aide de l'authentification adaptative en fonction des besoins de sécurité de mon organisation dans l'instance. La politique est-elle impactée par le mandat ?

   Non, si l'instance dispose déjà d'une stratégie de contexte Authentification adaptative - MFA active, la nouvelle stratégie MFA sécurisée par défaut n'est pas appliquée. Si la propriété MFA de l'instance était activée (glide.authenticate.multifactor), mais que la politique MFA n'était pas active, la politique MFA sécurisée par défaut permettant d'appliquer la MFA pour tous les utilisateurs internes (utilisateurs qui n'ont pas snc_external rôle) effectuant une connexion locale ou LDAP basée sur le nom d'utilisateur et le mot de passe est activée.

Exception d'application de la MFA

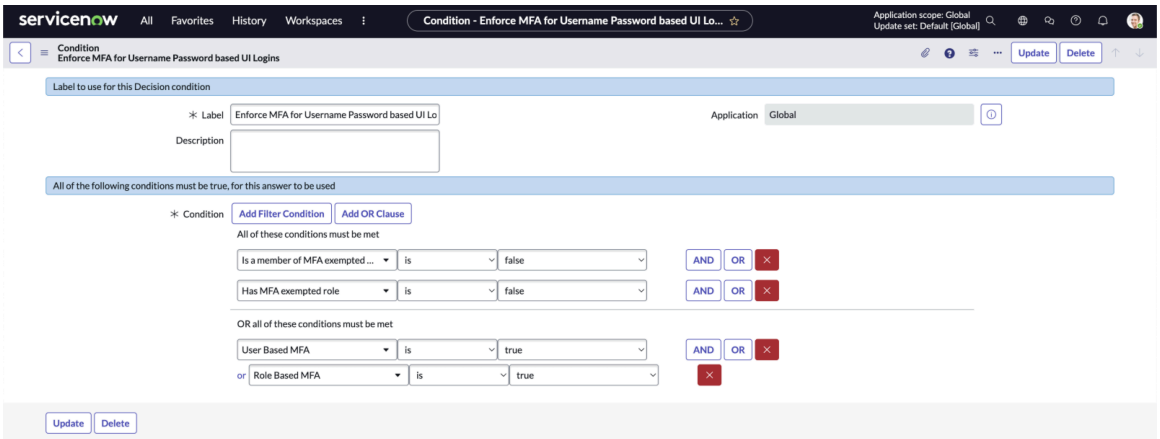
FAQ relative à l'exception d'application de la MFA et pourquoi c'est important.

1. Comment assouplir le mandat MFA pour des utilisateurs spécifiques ?

   Dans la version Yokohama, un nouveau groupe d'utilisateurs, un enregistrement de groupe d'utilisateurs exemptés de MFA est ajouté. Une politique MFA est ajoutée en fonction de la condition par défaut. Tout utilisateur membre de ce groupe est appliqué avec la MFA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour assouplir la MFA pour des utilisateurs spécifiques, suivez la procédure :

- Accédez au **contexte MFA**. La politique MFA ascendante associée à l'enregistrement de contexte MFA doit être « Appliquer la MFA pour les connexions non SSO.

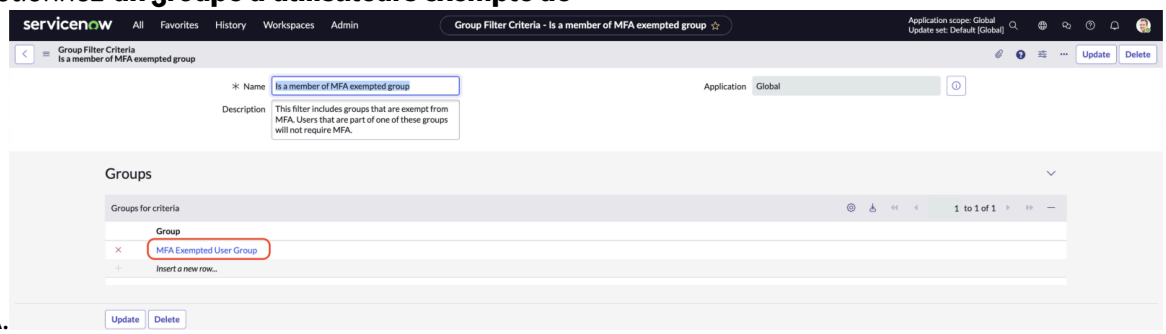


- Dans la liste connexe **Entrée de politique** , sélectionnez l'enregistrement **Est membre de Critères de filtre de groupe exempté de MFA** .

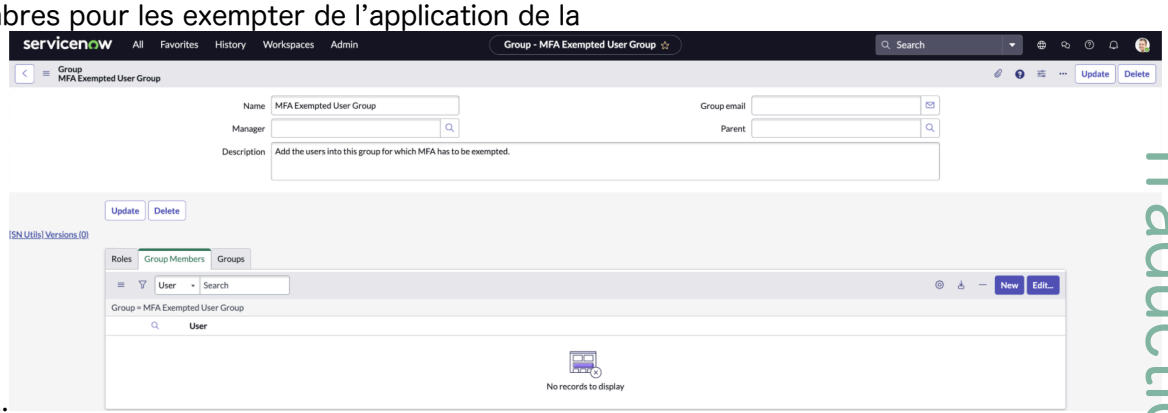
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélectionnez **un groupe d'utilisateurs exempté de MFA**.



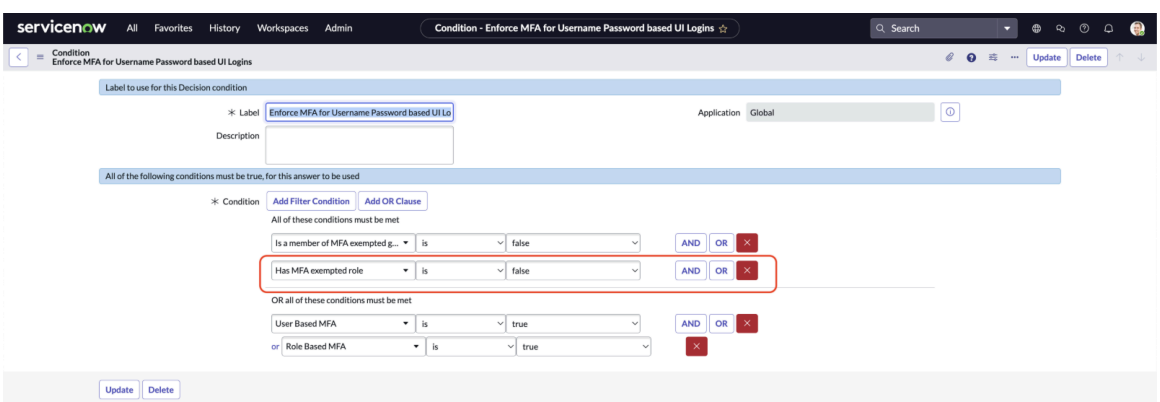
- Ajoutez des utilisateurs à ce groupe en tant que membres pour les exempter de l'application de la MFA.



Remarque :
Si vous avez une politique différente associée au contexte MFA, vous pouvez ajouter des critères de filtre « Est membre d'un groupe exempté de MFA » à votre politique et modifier les conditions de politique pour exempter les utilisateurs de ce groupe de l'application de la MFA.

2. Comment le mandat des AMF peut-il être assoupli pour certains rôles ?

Dans la version Yokohama, un nouveau critère de filtre de rôle **exempté de MFA** vide est ajouté. Des conditions ont été ajoutées à la politique MFA pour exempter de l'application de la MFA les utilisateurs qui font partie des critères de rôle exemptés.

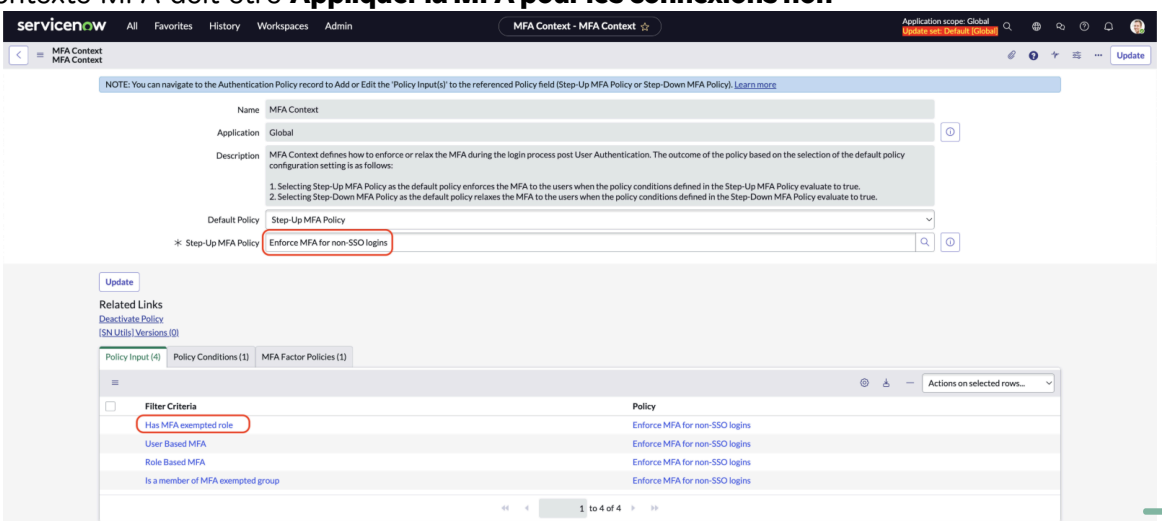


Pour assouplir la MFA pour des rôles spécifiques, suivez la procédure :

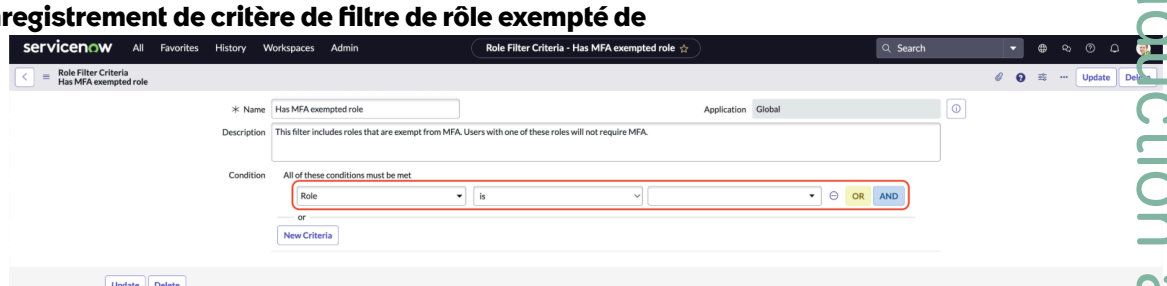
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Accédez au **contexte MFA**. La politique MFA ascendante associée à l'enregistrement de contexte MFA doit être **Appliquer la MFA pour les connexions non SSO**.



- Dans la liste connexe **Entrée de politique** , sélectionnez **A un enregistrement de critère de filtre de rôle exempté de MFA** .



- Ajoutez les rôles que vous souhaitez ajouter à la condition. Vous pouvez ajouter plusieurs rôles à l'aide de l'opérateur OU.

Remarque :
Si une politique différente est associée au contexte MFA, vous pouvez ajouter à votre politique des critères de filtre **A un rôle exempté de MFA** . Modifiez les conditions de politique pour exempter les utilisateurs ayant des rôles exemptés de l'application de la MFA.

3. Comment le mandat des AMF peut-il être assoupli pour certains groupes ?

Dans la version Yokohama, un **groupe d'utilisateurs exempté de MFA** est ajouté. Selon la condition par défaut ajoutée à la politique MFA, l'utilisateur ou le groupe qui est membre de ce groupe n'est pas appliqué avec la MFA.

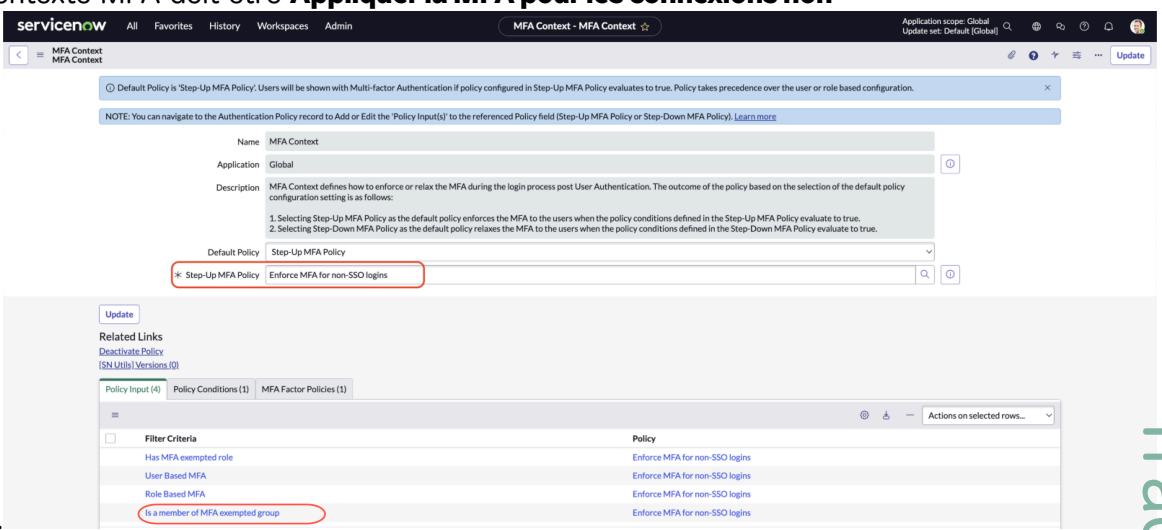


Traduction automatique

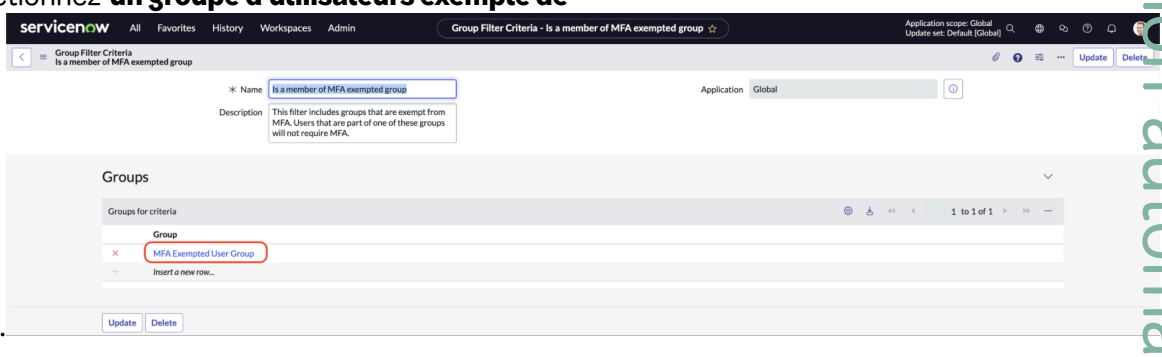
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour assouplir l'authentification multifacteur pour des groupes spécifiques, suivez la procédure :

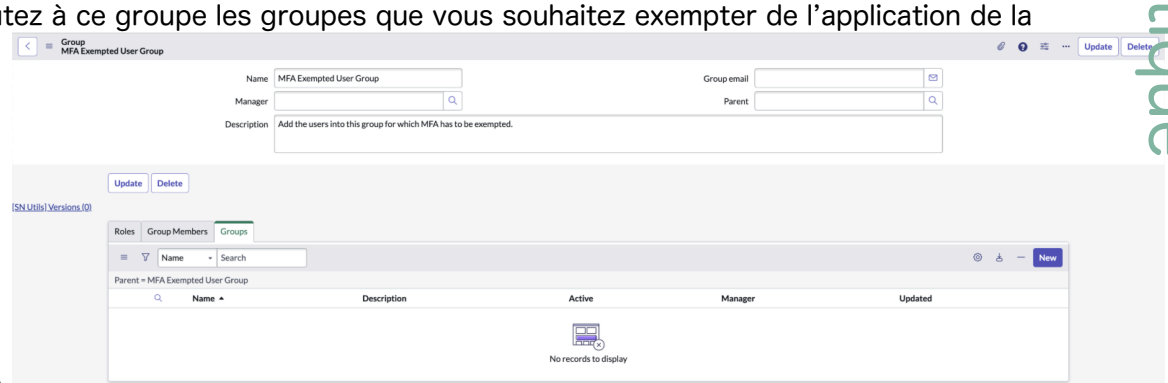
- Accédez au **contexte MFA**. La politique MFA ascendante associée à l'enregistrement de contexte MFA doit être **Appliquer la MFA pour les connexions non SSO**.



- Dans la liste connexe **Entrée de politique** , sélectionnez l'enregistrement **Est membre de Critères de filtre de groupe exempté de MFA** .
- Sélectionnez **un groupe d'utilisateurs exempté de MFA**.



- Ajoutez à ce groupe les groupes que vous souhaitez exempter de l'application de la MFA.



4. Comment assouplir le mandat des AMF pour les réseaux de confiance ?

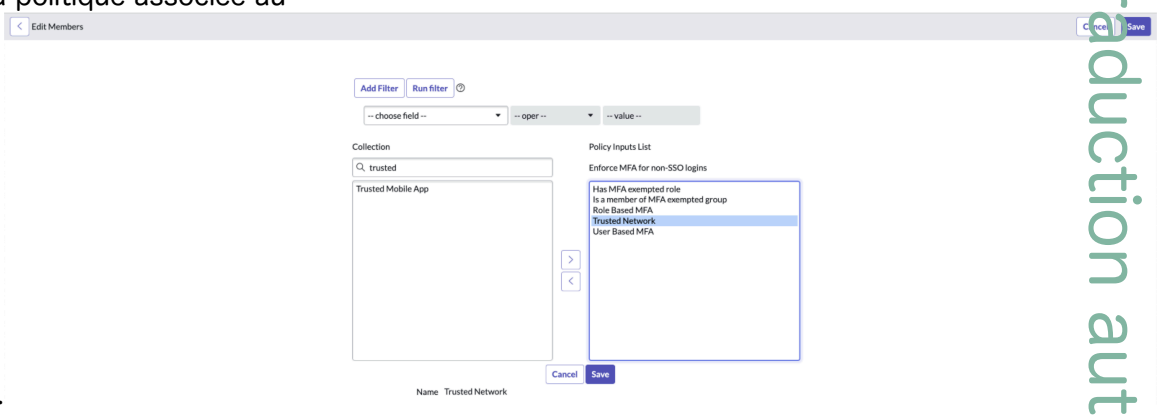
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Accédez à la **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre d'adresses IP**.
- Créez un critère pour spécifier un réseau approuvé. Vous pouvez spécifier une liste de plages IP ou de sous-réseaux dans le cadre du réseau approuvé.



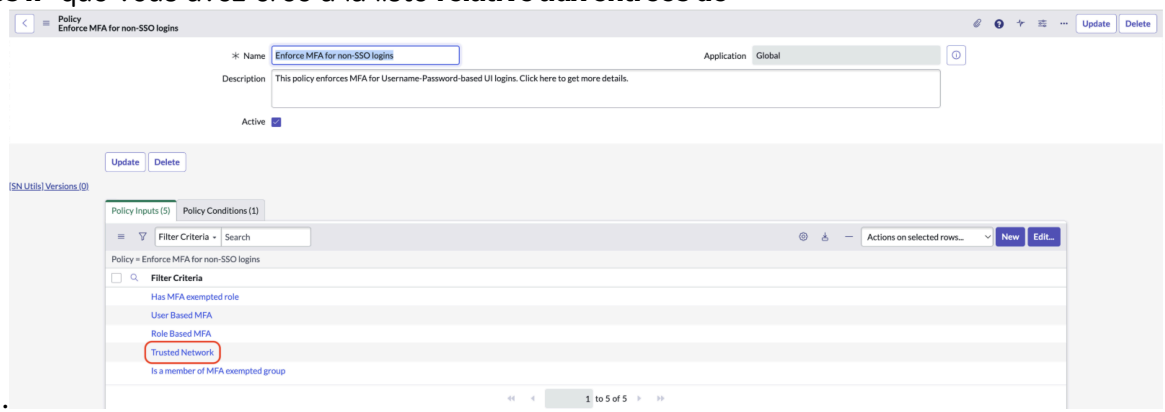
- Accédez à la **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte MFA**.
- Ouvrez la politique associée au contexte.



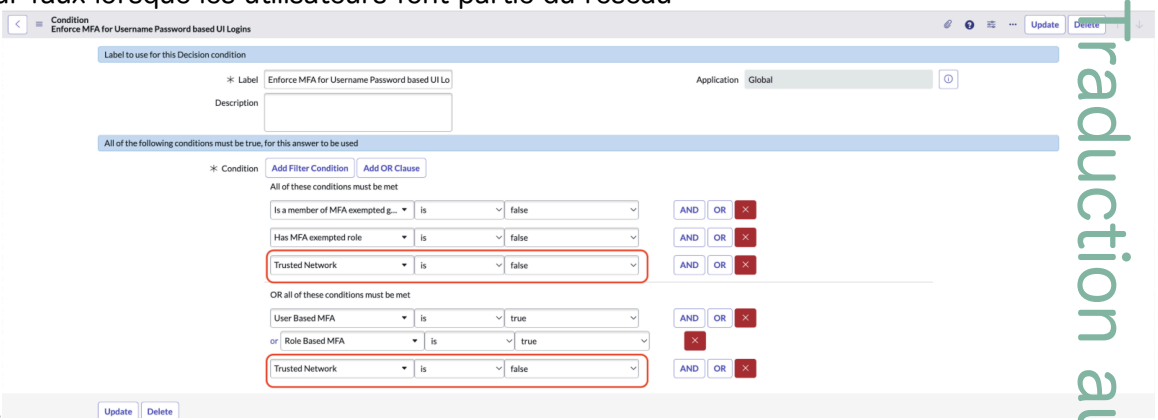
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélectionnez la modification pour ajouter le **critère de filtre d'adresses IP** que vous avez créé à la liste **relative aux entrées de politique** .



- Modifiez la condition de politique pour confirmer qu'elle est évaluée sur faux lorsque les utilisateurs font partie du réseau approuvé.



Remarque :
Si vous avez une politique différente associée au contexte MFA, vous pouvez ajouter les critères de filtre IP créés dans le cadre de l'étape 1 à votre politique et modifier les conditions de politique pour exempter l'application de la MFA sur le réseau approuvé.

5. Comment assouplir le mandat des MFA pour les sites de confiance ?

Vous pouvez utiliser les critères de filtre d'emplacement disponibles avec le module d'extension **Zero Trust - Accès basé sur l'emplacement** (nécessite un abonnement supplémentaire).

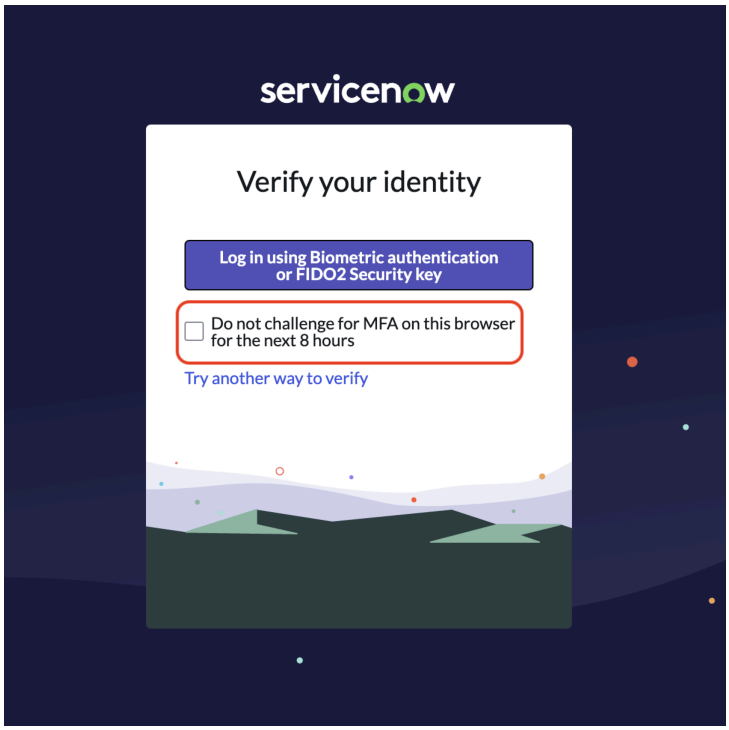
6. Comment contrôler l'application fréquente de la MFA ?

Utilisez les critères de filtre d'emplacement disponibles avec le module d'extension **Zero Trust - Accès basé sur l'emplacement** (nécessite un abonnement supplémentaire).

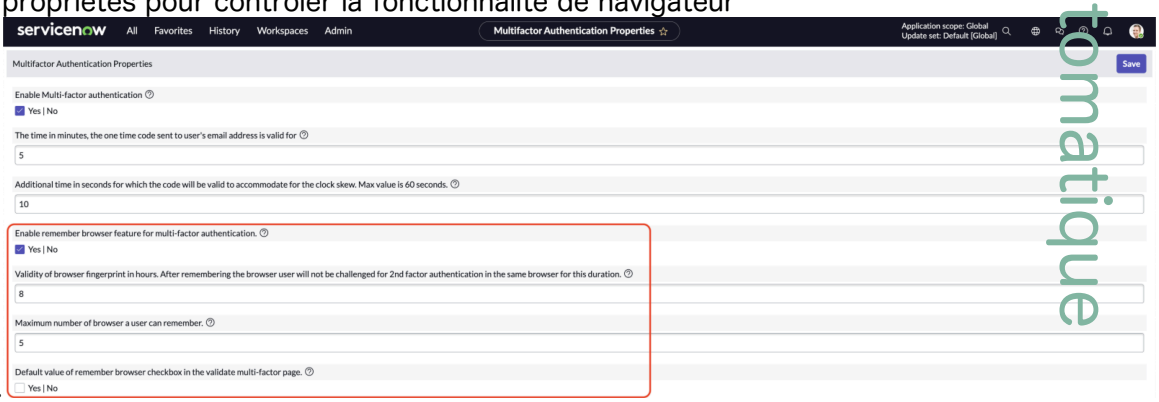
Sur la page de validation MFA, il y a une case à cocher pour mémoriser un navigateur. La MFA n'est pas appliquée sur le navigateur mémorisé :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- La durée spécifiée par cette propriété système. glide.authenticate.multifactor.browser.fingerprint.validity. La valeur par défaut de la propriété est de 8 heures. Cette durée peut être augmentée jusqu'à 24 heures. De même, à l'aide de la propriété système glide.authenticate.multifactor.remember.browser.default , la valeur par défaut de la case à cocher peut être définie sur vrai.
- Accédez à la **Authentification multifacteur** > **Propriétés** et ajustez ces quatre propriétés pour contrôler la fonctionnalité de navigateur mémorisée.



7. Comment fonctionne la MFA pour les comptes partagés par les utilisateurs ?

Les comptes uniques partagés par plusieurs utilisateurs constituent un risque pour la sécurité. Il n'est pas recommandé de partager un compte avec plusieurs utilisateurs.

Mesures MFA

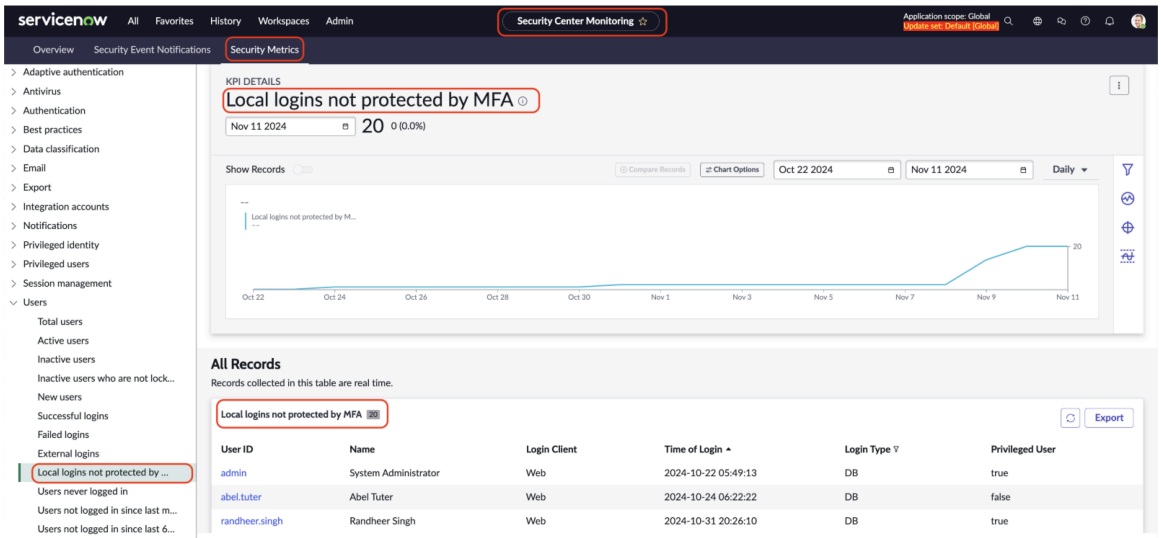
FAQ relative à la compréhension des mesures MFA.

1. Comment puis-je vérifier le nombre de connexions locales qui ne sont pas en cours de MFA ?

Vous pouvez accéder à **Centre de sécurité** > **Console de sécurité** > **Mesures de sécurité**. Sous Mesures pour les utilisateurs, cliquez sur connexion locale non protégée par MFA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Comment puis-je vérifier le nombre d'utilisateurs qui doivent encore terminer la configuration MFA et qui effectuent une connexion locale ?

Vous pouvez accéder à **Centre de sécurité** > **Console de sécurité** > **Mesures de sécurité**. Sous Mesures pour les utilisateurs, cliquez sur connexion locale non protégée par MFA.

Types de MFA

FAQ relative aux types de MFA et pourquoi c'est important.

1. Quels sont les types de méthodes de vérification disponibles pour la MFA ServiceNow?

ServiceNow Le système de base prend en charge ces méthodes de vérification.

a. Passe-partout

b. Applications d'authentification TOTP telles que Google Authenticator, Okta verify, Microsoft Authenticator, Authy, DUO

c. Authentificateur biométrique (FIDO2) tel que Windows Hello, Apple Touch ID, Face ID, capteur d'empreintes digitales Android.

d. Clés de sécurité matérielles (FIDO2) telles que YubiKey, Thetis

e. Mot de passe à usage unique (OTP) par e-mail

f. SMS OTP : l'authentification multifacteur avec SMS com.snc.authentication.sms_mfaplugin l'installation et la configuration du facteur sont requises pour activer l'authentification MFA basée sur SMS OTP.

2. Un utilisateur peut-il configurer plusieurs facteurs MFA ou méthodes de vérification ?

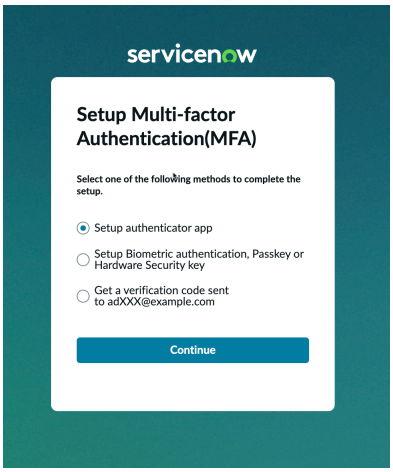
Oui, vous pouvez vous inscrire à plusieurs facteurs MFA en visitant leur profil d'utilisateur. Par exemple, vous pouvez inscrire un ordinateur portable avec l'authentificateur biométrique, utiliser le téléphone mobile avec une clé d'accès et configurer une application d'authentification.

3. Quelles étapes les utilisateurs doivent-ils effectuer pour terminer la configuration de la MFA ?

L'utilisateur peut effectuer l'une des options MFA suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Consultez la documentation pour en savoir plus sur la configuration de la Authentification multifacteur MFA.

4. La MFA basée sur SMS et e-mail OTP peut-elle être limitée à certains utilisateurs ?

   L'administrateur peut configurer des politiques de facteur MFA pour les facteurs MFA basés sur OTP e-mail et SMS afin de limiter ces facteurs à certains groupes d'utilisateurs ou rôles.

5. Les utilisateurs n'ont pas de téléphone portable où ils peuvent configurer une application d'authentification. Comment ces utilisateurs peuvent-ils activer la MFA ?

   À partir de la version Xanadu, vous pouvez utiliser un authentificateur biométrique, des clés d'accès, des clés de sécurité matérielles FIDO2 et une MFA basée sur OTP par e-mail sans nécessiter de configuration d'application d'authentification sur le téléphone mobile.

6. En tant qu'utilisateur final, comment configurer l'authentification multifacteur ?

   Consultez la documentation pour en savoir plus sur la configuration de la Utilisation de l'authentification multifacteur MFA.

Réinitialisation MFA

FAQ relative à la réinitialisation MFA et pourquoi c'est important.

1. Configuration de l'application d'authentification perdue. Comment puis-je réinitialiser ?

   Il est préférable que les utilisateurs s'inscrivent à plusieurs facteurs afin de ne pas être bloqués en raison de la MFA. Par exemple, vous pouvez disposer de l'application d'authentification TOTP, d'une clé d'accès et d'une MFA basée sur un OTP par e-mail.

   Si les utilisateurs ne sont pas en mesure d'utiliser l'un des facteurs de MFA inscrits, l'administrateur peut réinitialiser la MFA en suivant ces étapes.

   a. Effacement de la configuration de l'application d'authentification :
      - Accédez à la **Tous** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.
      - Recherchez l'utilisateur dans la table.
      - Supprimer l'enregistrement associé à l'utilisateur

   b. Effacement des authentificateurs et des clés d'accès FIDO2 :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Accédez à la **Tous** > **Authentification multifacteur** > **Authentification Web** > **Informations d'identification publiques de l'utilisateur**.
- Rechercher l'utilisateur dans la table
- Supprimer les enregistrements associés à l'utilisateur

c. Effacement des autres configurations multifacteurs associées à l'utilisateur

- Accédez à la **Tous** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.
- Rechercher l'utilisateur dans la table
- Supprimer les enregistrements associés à l'utilisateur

Au cas où personne, y compris l'administrateur, ne peut accéder à l'instance. L'administrateur peut effectuer une réinitialisation MFA en libre-service à l'aide d'un élément de catalogue disponible sur Now Support .

2. Comment éviter le verrouillage des administrateurs en raison de la MFA ?

Les administrateurs s'inscrivent pour plusieurs facteurs MFA afin de ne pas être empêchés d'accéder à l'instance.

Au cas où personne, y compris l'administrateur, ne peut accéder à l'instance. L'administrateur peut effectuer une réinitialisation MFA en libre-service à l'aide d'un élément de catalogue disponible sur Now Support .

Explorer l'authentification multifacteur

L'authentification multifacteur (MFA) est une méthode d'authentification qui demande aux utilisateurs de fournir des informations autres que leurs informations d'identification de base.

La MFA est un processus de sécurité qui nécessite qu'un utilisateur fournisse au moins deux facteurs de vérification différents pour accéder à un service ou à un compte. Il ajoute une couche de sécurité supplémentaire à votre service au-delà d'un simple mot de passe, ce qui rend plus difficile l'accès des personnes non autorisées.

En exigeant plusieurs facteurs, la MFA améliore considérablement la sécurité et aide à protéger contre diverses cybermenaces, notamment le phishing et l'usurpation d'identité. Voici un aperçu du fonctionnement de la MFA :

- **Premier facteur** : l'utilisateur utilise son nom d'utilisateur et son mot de passe pour se connecter.
- **Deuxième facteur** : l'utilisateur est invité à indiquer un deuxième facteur qui est avec l'utilisateur (une méthode de vérification d'identité telle qu'une application d'authentification ou une clé de sécurité).

En outre, ces facteurs peuvent généralement être classés en catégories sécurisées et moins sécurisées en fonction de leur niveau de protection contre les menaces de sécurité courantes.

- Facteurs garantis :
  - FIDO (Fast Identity Online) : ce facteur utilise des jetons matériels ou des méthodes d'authentification biométrique, offrant un haut niveau de sécurité en confirmant que l'utilisateur dispose d'un appareil physique ou d'un trait biométrique unique pour vérifier son identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **TOTP (mot de passe à usage unique basé sur le temps) :** Ce facteur génère un mot de passe à usage unique valide pendant une courte période, généralement 30 secondes. Il est généralement fourni via une application mobile, ajoutant une couche supplémentaire de sécurité en exigeant que l'utilisateur ait accès à un appareil et une application spécifiques.

- Facteurs moins garantis :
  - **MESSAGERIE ÉLECTRONIQUE:** Ce facteur envoie un code de vérification ou un lien à l'adresse e-mail de l'utilisateur. Bien que pratique, il est moins sécurisé car les comptes de messagerie peuvent être compromis.
  - **SMS:** Ce facteur envoie un code de vérification par SMS au numéro de téléphone de l'utilisateur. Il est également moins sécurisé en raison du potentiel d'échange de cartes SIM et d'autres vulnérabilités des téléphones portables.

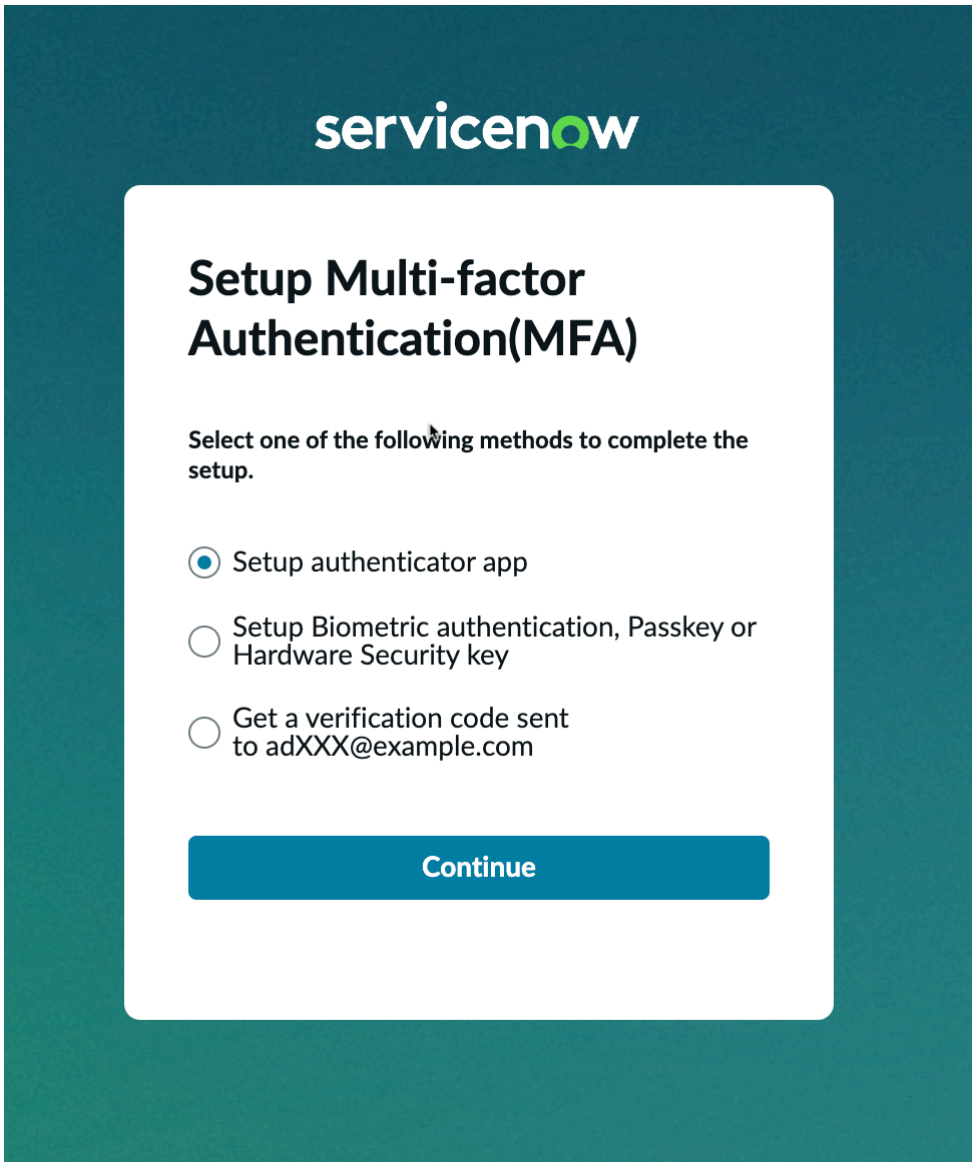
Pour renforcer la sécurité, il est recommandé de privilégier l'utilisation de facteurs sécurisés tels que FIDO et TOTP par rapport à des facteurs moins sécurisés tels que les e-mails et les SMS.

Remarque :

- La MFA est activée par défaut sur ServiceNow.
- La MFA est activée à l'aide de la `glide.authenticate.multifactor` propriété. Si vous souhaitez désactiver cette propriété, vous devez fournir une justification commerciale expliquant pourquoi vous souhaitez désactiver la MFA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

ServiceNow La MFA de prend en charge les méthodes de vérification telles que l'application d'authentification, la FIDO2 (Fast IDentity Online 2), la clé d'accès et le mot de passe à usage unique (OTP) basé sur le temps. Les méthodes de vérification disponibles sont décrites ci-dessous :

- **Application d'authentification** : applications qui génèrent des codes de vérification uniques et temporaires. Par exemple : Okta, Google Authenticator, Microsoft Authenticator, etc.
- **FIDO2** : appareils physiques qui utilisent la cryptographie à clé publique pour valider les identités des utilisateurs. Par exemple : clés matérielles (YubiKey), scanners biométriques (Touch ID d'Apple).
- **Clé d'accès** : connectez-vous avec une clé d'accès en déverrouillant l'appareil à l'aide d'un capteur biométrique, d'un code PIN ou d'un modèle.
- **OTP** : la clé secrète et l'heure actuelle pour générer un mot de passe unique qui n'est valide que pour une courte période. Par exemple : SMS (OTP) et e-mail (OTP).

Vous pouvez utiliser l'authentification multifacteur avec les éléments suivants :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Authentification de base de données locale (authentification native ServiceNow) ou Intégration du protocole LDAP
- SSO SAML ou SSO OIDC. Pour plus d'informations, consultez Authentification unique (SSO) de plusieurs fournisseurs.

Information associée

Méthodes de vérification de l'authentification multifacteur

Propriétés système de l'authentification multifacteur

Configuration de l'authentification multifacteur

Configurez l'authentification multifacteur (MFA) pour améliorer la posture de sécurité de vos utilisateurs lors de l'utilisation de ServiceNow.

Tout d'abord, pour mettre en œuvre l'authentification multifacteur, déterminez les méthodes de vérification de l'authentification multifacteur en fonction des besoins de l'entreprise et des utilisateurs.

Après avoir identifié les besoins, avec ServiceNow l'authentification multifacteur de , vous pouvez sélectionner la bonne méthode ou la combinaison de celle-ci pour vos utilisateurs. En outre, vous pouvez également utiliser les différentes propriétés d'authentification multifacteur pour activer, désactiver et configurer l'authentification multifacteur afin d'améliorer davantage l'expérience MFA de l'utilisateur en fonction des critères d'authentification.

Voici quelques-uns des sujets importants liés à la configuration de l'authentification multifacteur :

- Méthodes de vérification de l'authentification multifacteur
- Propriétés système de l'authentification multifacteur
- Critères d'authentification multifacteur

Contexte d'authentification multifacteur

Le contexte politique de l'authentification multifacteur (MFA) utilise une stratégie pour définir comment et quand la MFA est appliquée pendant le processus de connexion.

Enregistrement de contexte MFA

Le contexte de la politique MFA définit si vos utilisateurs doivent fournir une deuxième forme d'authentification lorsqu'ils se connectent. Ce contexte ne refuse pas l'accès à votre instance comme les politiques de post-authentification et de pré-authentification. La politique que vous sélectionnez dans ce contexte a priorité sur les configurations basées sur l'utilisateur ou les rôles pour l'authentification multifacteur.

Pour accéder au contexte MFA, accédez à **Tous** > **Authentification multifacteur** > **Contexte MFA**.

Utilisez les champs dans l'enregistrement de contexte de la politique de post-authentification pour définir la façon dont votre instance utilise votre stratégie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si la politique par défaut est **une politique MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans **la politique MFA** ascendante est évaluée comme vraie. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.
- MFA avec connexion SSO n'est disponible que si la propriété glide.authenticate.mfa.with.multisso.enabled est définie sur vrai.
- Vous pouvez accéder à l'enregistrement Politique d'authentification pour ajouter ou modifier les « entrées de la politique » au champ de politique référencé (**Politique de MFA ascendante** ou **Politique de MFA descendante**).
- La politique de contexte MFA s'applique uniquement aux connexions des utilisateurs. Cela ne s'applique pas à l'authentification API, à l'authentification de base et à l'octroi des informations d'identification du mot de passe du propriétaire de ressource OAuth.

Formulaire de contexte MFA

Champ	Description
Nom	Nom du contexte de politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Politique MFA ascendante** Applique la MFA aux utilisateurs lorsque les conditions de politique définies dans le champ **Politique de MFA ascendante** sont évaluées sur vrai. **Politique MFA descendante** Applique la MFA par défaut. La MFA n'est pas appliquée uniquement lorsque les conditions de politique définies dans le champ **Politique de MFA descendante** sont évaluées comme vraies.
Politique MFA ascendante	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA** ascendante.
Politique MFA descendante	La politique utilisée dans ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA descendante**.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Politique de MFA ascendante** ou **Politique de MFA descendante** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône de référence (icône ⓘ) en regard du champ **Politique de MFA ascendante** ou **Politique de MFA descendante** .

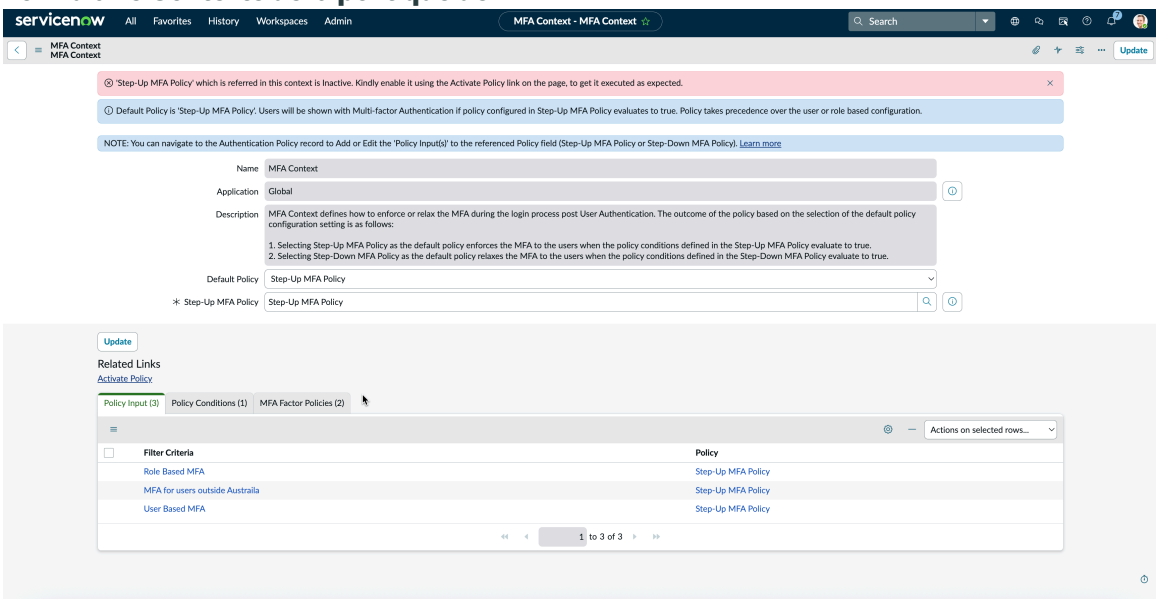
Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais en tant que bonne pratique, il est recommandé d'ajouter de nouvelles conditions de politique à partir de la page de politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet exemple montre un enregistrement de contexte MFA configuré à l'aide d'une politique MFA ascendante. Cette politique par défaut signifie que la MFA n'est appliquée que lorsque les conditions définies dans la politique sont évaluées comme vraies. Le contexte utilise une politique appelée **politique MFA Step-Up**. Cette politique comporte un ensemble d'entrées et de conditions qui sont affichées dans les onglets **Entrée de politique** et **Condition de politique** .

Formulaire Contexte de la politique de MFA



Politiques de facteur MFA

Les politiques de facteur MFA sont un élément essentiel de la posture de sécurité d'une organisation, vous permettant d'appliquer des étapes de vérification supplémentaires au-delà des mots de passe. Ces politiques définissent les méthodes d'authentification auxquelles les utilisateurs doivent accéder, offrant ainsi une approche flexible et personnalisable de l'authentification. Pour plus d'informations, consultez Politiques de facteur d'authentification multifacteur.

Méthodes de vérification de l'authentification multifacteur

ServiceNow MFA de prend en charge les méthodes de vérification telles que l'application d'authentification, la FIDO2 (Fast IDentity Online 2) et le protocole TOTP (Time-based One-time Password).

Les utilisateurs peuvent utiliser les options suivantes en plus de leur nom d'utilisateur et de leur mot de passe pour répondre aux exigences d'authentification multifacteur. Les utilisateurs peuvent configurer indépendamment des facteurs MFA tels que les applications d'authentification, les scanners biométriques, les clés matérielles et les SMS.

Applications d'authentification

Une application d'authentification est un logiciel tiers qui génère des codes d'accès temporaires. Les utilisateurs peuvent utiliser ces codes secrets avec leur mot de passe pour se connecter à une instance qui nécessite l'authentification multifacteur (MFA). Pour en savoir plus sur ces applications, reportez-vous à la section Applications d'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Clés matérielles et scanners biométriques (authentification Web)

Le module d'extension *`Integration - Web Authentication`* (com.snc.integration.webauthn) permet l'authentification par clé matérielle ou lecteur biométrique sur votre instance.

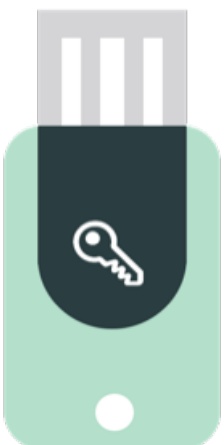
Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.



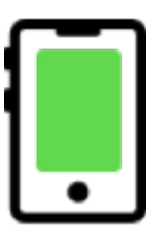
Passe-partout

L'authentification par clé d'accès est une méthode de connexion sécurisée et sans mot de passe, où les utilisateurs utilisent une clé d'accès en déverrouillant leur appareil avec un capteur biométrique, un code PIN ou un modèle.

SMS

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de se connecter à l'instance à l'aide d'un OTP basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP SMS est envoyé au numéro de téléphone portable associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité. Pour plus d'informations, consultez SMS en tant que facteur MFA.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

E-mail

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un e-mail.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP e-mail est envoyé à l’adresse e-mail de l’utilisateur. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu’ils ont envoyé à l’adresse e-mail et vérifier leur identité. Pour plus d'informations, consultez L’e-mail en tant que facteur MFA.



Information associée

- Authentification Web - MFA
- Méthodes de vérification de l’authentification multifacteur
- L’e-mail en tant que facteur MFA

Authentification Web - MFA

Utilisez **Intégration - Authentification Web (com.snc.integration.webauthn)** pour autoriser l’authentification par clé matérielle ou par lecteur biométrique sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.



Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

Configuration de l'authentification multifacteur avec la biométrie

Les administrateurs peuvent utiliser la liste des informations d'identification publiques de l'utilisateur pour afficher et gérer les informations d'identification créées par l'utilisateur.

Lorsqu'un utilisateur enregistre une application d'authentification, une authentification biométrique ou une clé matérielle, votre instance crée un enregistrement dans la table

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification publiques de l'utilisateur[sys_user_public_credential]. Utilisez cette table pour voir quels utilisateurs ont enregistré un authentificateur, ainsi que leurs types et quand ils ont été enregistrés et utilisés. Vous pouvez également marquer ces enregistrements comme inactifs pour empêcher les informations d'identification d'empêcher les utilisateurs d'utiliser ces informations d'identification.

Le module **d'extension Intégration - Authentification Web (com.snc.integration.webauthn)** doit être activé pour l'authentification Web (FIDO2).

Remarque :
Le module **d'extension Intégration - Authentification Web (com.snc.integration.webauthn)** est installé par défaut.

Formulaire d'informations d'identification publiques de l'utilisateur

Champ	Description
Pseudonyme des informations d'identification	Surnom de l'information d'identification. Ce surnom est choisi par l'utilisateur lors de l'enregistrement d'un authentificateur.
Utilisateur	Utilisateur associé aux informations d'identification
Actif	Indique si l'identifiant est actif. Les administrateurs peuvent définir un enregistrement sur inactif pour empêcher un utilisateur de s'authentifier avec ces informations d'identification.
Authentificateur	Type d'authentificateur enregistré par l'utilisateur.
Heure d'inscription	Date et heure auxquelles l'utilisateur a créé ces informations d'identification
Heure de la dernière utilisation	Date et heure auxquelles l'utilisateur s'est connecté pour la dernière fois avec ces informations d'identification.

Types d'authentificateur restreints

Si vous avez restreint une méthode d'authentification, telle que les authentificateurs biométriques, les utilisateurs ne seront pas en mesure de créer de nouvelles informations d'identification de ce type. Toutefois, toutes les informations d'identification créées avant l'application de cette restriction continueront de fonctionner. Vous pouvez désactiver les enregistrements de la table Informations **d'identification publiques de l'utilisateur** pour empêcher l'utilisation de ces informations d'identification après leur création.

Options de configuration de l'authentificateur

Utilisez la page Configuration de l'authentificateur pour gérer les options d'authentification sur votre instance.

Accédez à la **Authentification multifacteur** > **Authentification Web** > **Configuration de l'authentificateur** pour afficher et modifier les options de configuration par défaut.

Formulaire de configuration de l'authentificateur

Champ	Description
Type d'authentificateur autorisé	Type d'authentificateurs autorisés à être enregistrés. Sélectionner à partir de :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de configuration de l'authentificateur (suite)

Champ	Description
	• Les authentificateurs **de plateforme** sont attachés ou intégrés à un appareil. Les lecteurs d'empreintes digitales ou la reconnaissance faciale disponibles sur les appareils mobiles (tels que Apple FaceID ou TouchID) entrent dans cette catégorie. • Les authentificateurs **itinérants** peuvent être supprimés d'un ordinateur ou d'un autre appareil client et utilisés ailleurs. Les clés matérielles entrent dans cette catégorie.
Type d'attestation	Définir la valeur sur direct ou indirect requiert l'importation des métadonnées d'authentificateur pour attester la provenance d'un authentificateur pendant l'enregistrement. • Aucun • Direct • Indirect
Auto-attestation de plateforme	Indique si l'auto-attestation est activée pour les authentificateurs de plateforme.
Auto-attestation multiplateforme	Indique si l'auto-attestation est activée pour les authentificateurs itinérants.
Vérification de l'utilisateur	Sélectionnez **Préféré** ou **Obligatoire**. Si nécessaire, le flux d'authentification Web invite les utilisateurs à vérifier à l'aide d'un code PIN ou biométrique.
Vérifier la présence de l'utilisateur	Indique si le flux d'authentification Web nécessite la vérification de présence de l'utilisateur.
Clé de résident	Sélectionnez **Préféré** ou **Obligatoire**. Si nécessaire, l'authentificateur conserve les informations d'identification de clé publique dans le stockage de l'authentificateur.
Délai d'expiration (en ms)	Limite de temps maximale pour terminer l'enregistrement et l'authentification Web. Le temps est en millisecondes.

Politiques de facteur d'authentification multifacteur

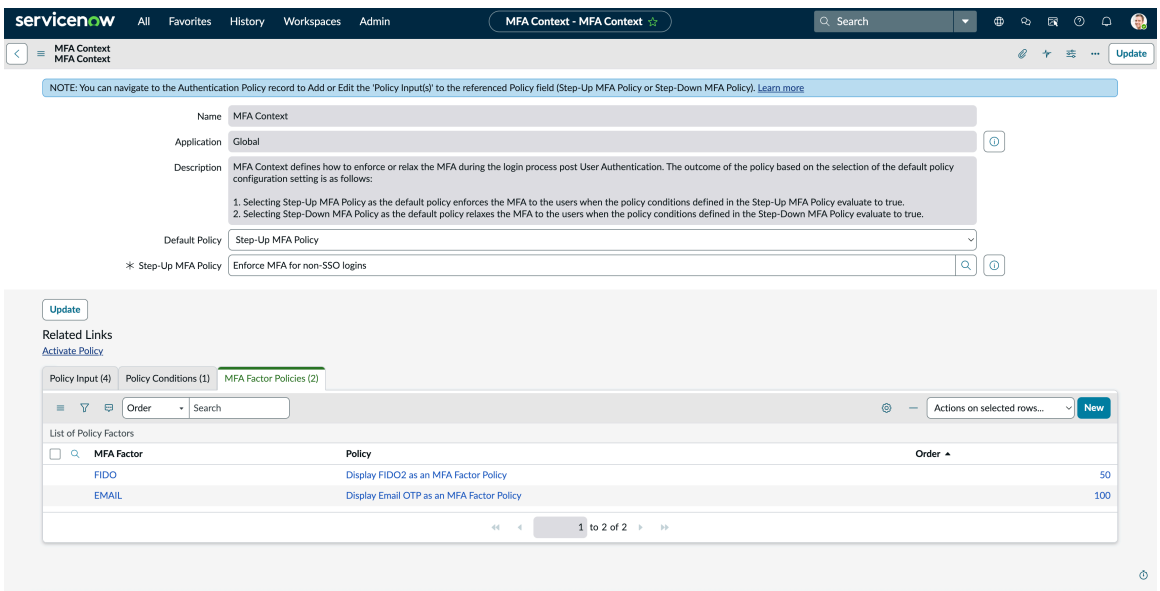
Utilisez les politiques de facteur MFA pour spécifier les types de facteurs d'authentification que vous souhaitez autoriser pour votre instance.

Les politiques de facteur MFA sont un élément essentiel de la posture de sécurité d'une organisation, vous permettant d'appliquer des étapes de vérification supplémentaires au-delà des mots de passe. Ces politiques définissent les méthodes d'authentification que les utilisateurs doivent utiliser pour accéder aux ressources de votre organisation, offrant ainsi une approche flexible et personnalisable de l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La mise en œuvre de politiques de facteur MFA est essentielle pour améliorer la sécurité des systèmes et des données de votre organisation. Ces stratégies fournissent une couche supplémentaire de protection contre les cybermenaces, ce qui rend plus difficile pour les attaquants d'obtenir un accès non autorisé.



Pour utiliser les politiques de facteur MFA, vous devez configurer les entrées et conditions de politique ainsi qu'un contexte MFA. Pour en savoir plus, reportez-vous à la section Contexte d'authentification multifacteur.

Voici les politiques de facteur MFA disponibles dans ServiceNow lesquelles vous pouvez spécifier les types de facteurs d'authentification autorisés ou requis :

- FIDO2
- SMS
- E-mail

Pour tirer le meilleur parti des politiques de facteur MFA, vous devez comprendre comment les configurer et les gérer efficacement. Cela inclut la définition des méthodes d'authentification, la spécification des entrées et des conditions de la politique et la configuration de l'application de la politique (contexte MFA). En comprenant et en mettant en œuvre les politiques de facteur MFA, vous pouvez améliorer considérablement la sécurité et l'intégrité des systèmes et des données de votre organisation.

Information associée

Contexte d'authentification multifacteur

FIDO2 comme facteur MFA

SMS en tant que facteur MFA

L'e-mail en tant que facteur MFA

FIDO2 comme facteur MFA

Vous pouvez configurer FIDO2 en tant que politique de facteur MFA pour appliquer la MFA pour la vôtre.

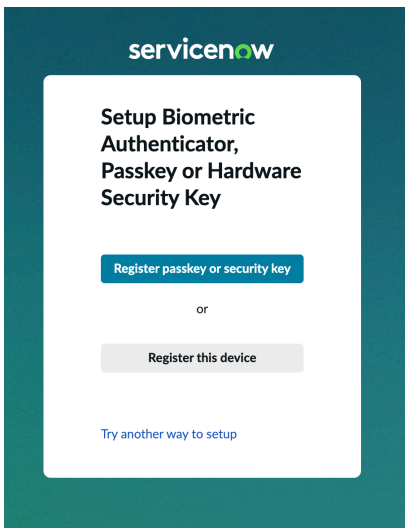
FIDO2 est une norme d'authentification sans mot de passe qui permet aux utilisateurs de s'authentifier à l'aide d'une clé de sécurité physique ou d'une authentification biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il offre une alternative plus sûre aux méthodes MFA traditionnelles, réduisant le risque de phishing et d'autres cyberattaques.

L'amélioration de la politique de facteur FIDO2 fournit une méthode d'authentification sécurisée pour vos politiques d'authentification multifacteur (MFA). Vous pouvez configurer FIDO2 en tant qu'option de politique de facteur MFA, offrant un niveau de sécurité supérieur par rapport aux méthodes traditionnelles telles que les e-mails et les SMS.



Vous pouvez configurer la politique de facteur FIDO2 et lorsque les utilisateurs satisfont à la condition de politique de facteur, la configuration FIDO2 s'affiche pendant la connexion à ServiceNow, pour les utilisateurs qui n'ont pas encore ajouté de clé matérielle ou biométrique enregistrée sur leur profil.

Si l'enregistrement est terminé, un écran de validation du deuxième facteur s'affiche pour vous connecter.

Remarque :
FIDO2 peut également être auto-inscrit par les utilisateurs. Pour en savoir plus sur la façon de s'inscrire automatiquement, consultez Configurer l'authentification multifacteur sur votre profil d'utilisateur.

Principaux avantages

Voici quelques-uns des principaux avantages de l'utilisation de FIDO2 en tant que facteur MFA :

Authentification FIDO2 exclusive

Assurez-vous que les comptes à privilèges élevés ne peuvent s'authentifier qu'à l'aide des capacités d'authentification forte de FIDO2 (biométrie, clés d'accès ou clés de sécurité matérielles).

Exclusion des méthodes moins sécurisées

Supprimez les autres méthodes d'authentification lorsque FIDO2 est la seule politique correspondante.

Inscription forcée

Exigez des utilisateurs qu'ils enregistrent une clé FIDO2 s'ils ne sont pas déjà inscrits.

Contrôle granulaire

Appliquez une application stricte à des rôles ou à des groupes spécifiques à l'aide du ciblage basé sur des politiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En tant que facteur de sécurité plus élevé, FIDO2 dispose de capacités exclusives d'application de la loi. Lorsqu'il s'agit de la seule politique correspondante pour un utilisateur :

- Remplace les autres facteurs d'inscription.
- Force l'inscription FIDO2 si l'utilisateur n'est pas inscrit.
- Devient l'option d'authentification exclusive.

Exemples de configurations et de comportements d'utilisateur

La table suivante illustre la manière dont les différents scénarios d'utilisateurs sont gérés en fonction de leurs rôles et facteurs d'inscription.

Exemple d'utilisateur	A des rôles	Facteurs déjà inscrits	Politiques correspondantes	Comportement
andrew.och	**ITIL**	Aucun	FIDO2	L'utilisateur est redirigé vers la configuration MFA avec FIDO2 uniquement. Après l'inscription, FIDO2 est la seule option d'authentification.
abel.tuter	**ITIL**	Authentificateur	FIDO2	L'utilisateur est redirigé vers la configuration MFA avec FIDO2 uniquement, même s'il dispose de l'authentificateur comme facteur d'auto-inscription. **Remarque :** Si l'utilisateur ne s'est inscrit à aucun facteur MFA, il est redirigé vers la configuration MFA avec FIDO2.
aileen.motterm	**ATOUT**	Authentificateur	E-mail	Voit les options d'e-mail et d'authentification pendant la connexion. L'utilisateur peut choisir l'un ou l'autre facteur ou éventuellement enregistrer FIDO2.
Abraham.Lincoln	**ACTIF,ITIL**	Authentificateur	E-mail et FIDO2	Voit l'option d'e-mail et d'authentificateur pendant la connexion. L'utilisateur peut enregistrer FIDO2 pendant la validation. Après l'inscription, l'utilisateur peut voir les 3 facteurs.

En configurant FIDO2 en tant que politique de facteur MFA, vous pouvez améliorer considérablement la sécurité de vos processus d'authentification.

Configurer FIDO2 en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher FIDO2 en tant que politique de facteur MFA pour l'authentification.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

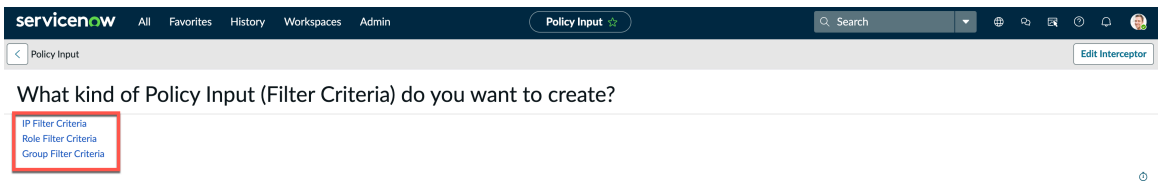
Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Contexte MFA**.
2. Sélectionnez l'onglet **Politiques de facteur MFA** .
3. Sélectionnez **Afficher FIDO2 comme politique de facteur MFA**.
4. Sélectionnez **Nouveau** pour ajouter des **entrées de politique**.
5. Sélectionnez les critères de filtre que vous souhaitez créer.

   Les types de critères de filtre sont les suivants :

   - Critère de filtre d'adresses IP
   - Critère de filtre de rôle
   - Critère de filtre de groupe

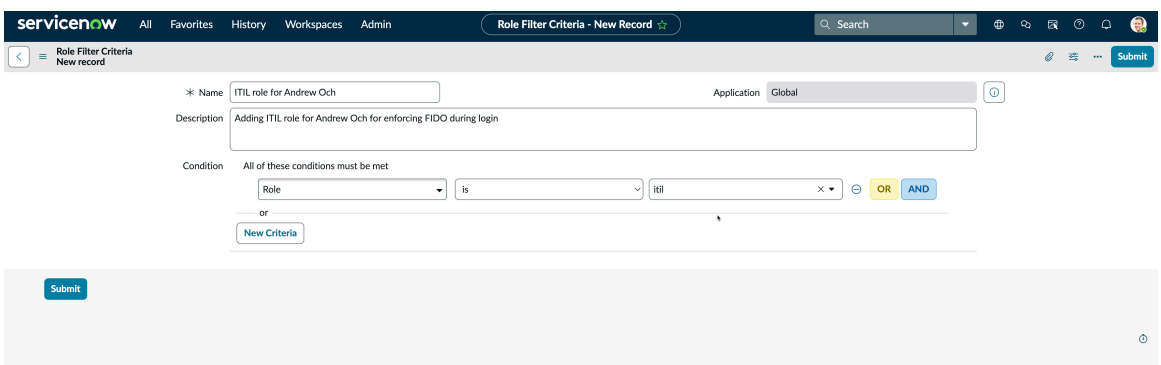
   Par exemple, Critères de filtre de rôle.



6. Sélectionnez **Critères de filtre de rôle**, renseignez les champs correspondant aux critères de filtre de rôle et envoyez l'enregistrement.

   La nouvelle politique est créée. Pour plus d'informations, consultez Critères de filtre de rôle.

   Prenons un exemple d'utilisation du rôle **ITIL** pour l'utilisateur (**andrew.och**) en tant qu'entrée de politique et soumettons.



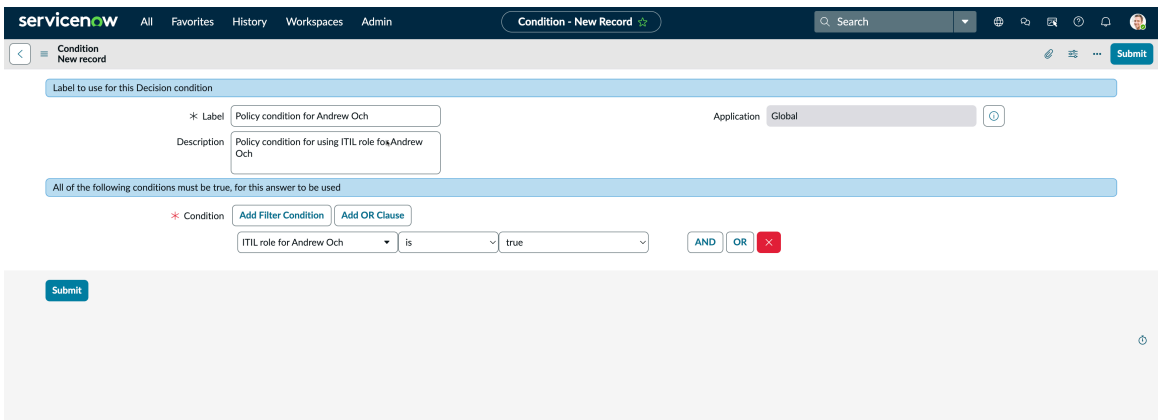
7. Sur la page Politique - Afficher FIDO2 en tant que politique de facteur MFA, sélectionnez **Conditions de politique**.
8. Sélectionnez **Nouveau** pour ajouter des conditions de politique.
9. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

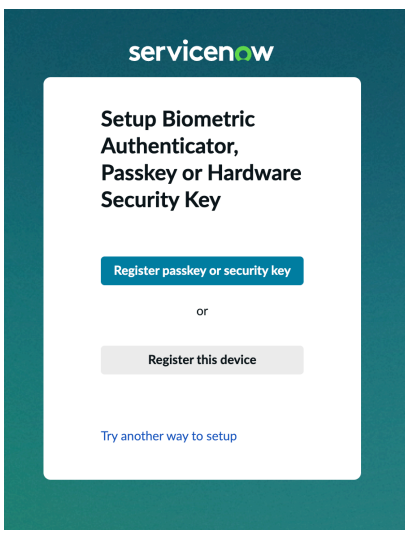
Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtre) utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basés sur les rôles qui a été créée pour la condition.



10. Sélectionnez **Soumettre**.

En fonction de l'entrée et de la condition de la politique, si l'utilisateur (**andrew.och**) tente de se connecter à l'instance, il s'affiche sous la forme d'un écran FIDO pour s'inscrire et s'inscrire.



Pour en savoir plus sur les différents exemples de configuration et les comportements utilisateur, reportez-vous à la section Exemples de configurations et de comportements d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. **Facultatif :** Répétez l’étape 8 pour créer des conditions de politique supplémentaires.

> **Remarque :**
> Si vous créez plusieurs conditions de politique, le résultat final de la politique d’accès dépend de la sortie logique OU de toutes les conditions de politique. En fonction des conditions, la politique est évaluée.

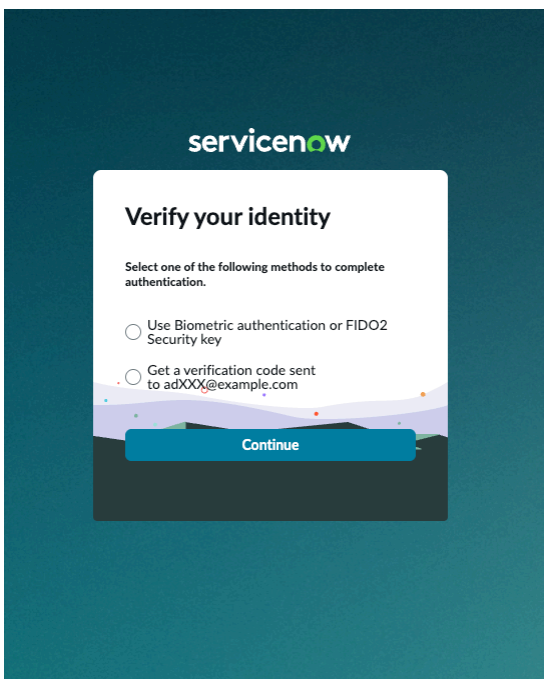
SMS en tant que facteur MFA

Authentification multifacteur (MFA) avec SMS comme facteur d’authentification.

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par SMS est envoyé au numéro de téléphone mobile associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

Vous pouvez également configurer la MFA avec SMS à l’aide de l’interface prête à l’emploi Twilio . Pour plus d'informations, consultez Fournisseurs d’authentification multifacteur.



En outre, l’authentification multifacteur avec SMS peut être contrôlée en fonction des entrées et des conditions de la politique à l’aide de critères de filtrage. Les types de critères de filtre sont les suivants :

- Critère de filtre d'adresses IP
- Critère de filtre de rôle
- Critère de filtre de groupe

Activer le module d’extension MFA with SMS

Pour MFA avec SMS, installez le module d’extension Authentification multifacteur avec SMS (com.snc.authentication.sms_mfa).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Les éléments suivants sont installés avec l'authentification multifacteur par SMS :

- Authentification adaptative (com.snc.adaptive_authentication
- Notification - Pilote Twilio Direct (com.snc.notify.twilio_direct)

Module d'extension dépendant : Intégration - Authentification multifacteur (com.snc.integration.multifactor.authentication)

Remarque :
Vous pouvez charger les données de démonstration lors de l'installation du module d'extension si vous configurez un fournisseur personnalisé pour générer le SMS.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Authentification multifacteur avec SMS (com.snc.authentication.sms_mfa) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Configurer SMS en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher le mot de passe à usage unique du SMS en tant que politique de facteur MFA pour l'authentification.

Avant de commencer
Module d'extension requis : authentification multifacteur avec SMS (com.snc.authentication.sms_mfa).

Rôle requis : admin

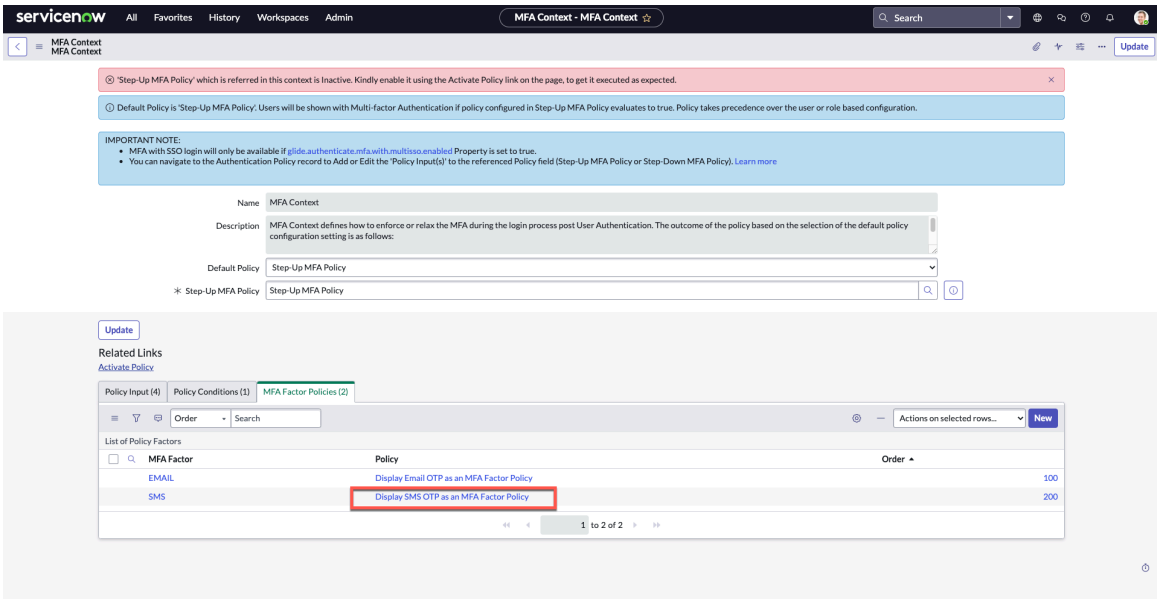
Remarque :
La politique de contexte MFA doit être évaluée comme vraie pour appliquer la politique de facteur SMS.

Procédure

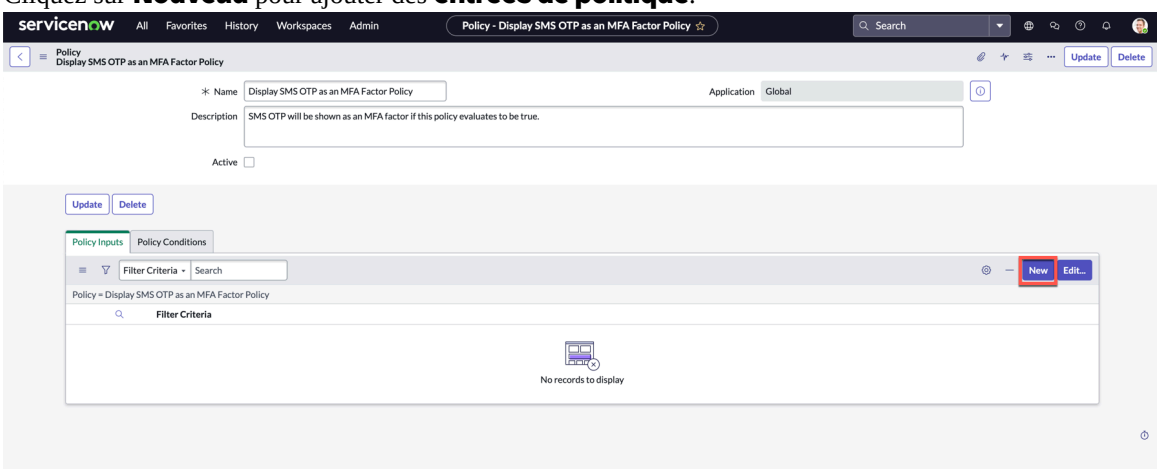
1. Accédez à la **Tous** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur l'onglet **Politiques de facteur MFA** .
3. Sélectionnez **Afficher le mot de passe à usage unique SMS comme politique de facteur MFA**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Nouveau** pour ajouter des **entrées de politique**.

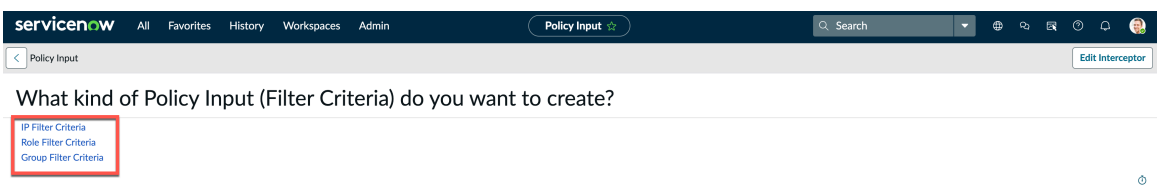


5. Sélectionnez les critères de filtre que vous souhaitez créer.

Les types de critères de filtre sont les suivants :

- Critère de filtre d'adresses IP
- Critère de filtre de rôle
- Critère de filtre de groupe

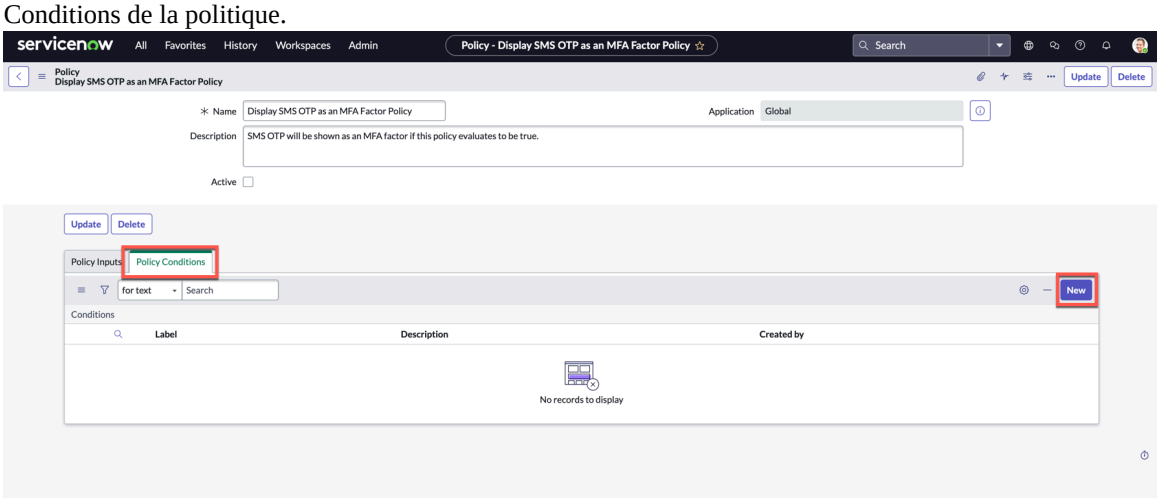
Par exemple, Critères de filtre de rôle.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Critères de filtre de rôle**, renseignez les champs correspondant aux critères de filtre de rôle et envoyez l'enregistrement.
   La nouvelle politique est créée. Pour plus d'informations, consultez Critères de filtre de rôle.
7. Sur la page Politique - Afficher le mot de passe OTP SMS en tant que politique de facteur MFA, cliquez sur Conditions de la politique.



8. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
9. Remplissez les champs du formulaire.

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtre) utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basés sur les rôles qui a été créée pour la condition.

10. Cliquez sur **Envoyer**.
11. **Facultatif :** Répétez l'étape 8 pour créer des conditions de politique supplémentaires.

> **Remarque :**
> Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la politique est évaluée sur vrai si l'une de vos conditions de politique est remplie.

En fonction de la politique de filtre de rôle (utilisateurs) et de la correspondance des conditions spécifiées pour le rôle, le SMS en tant que facteur MFA est affiché comme une option d'authentification pour les utilisateurs.

Fournisseurs d'authentification multifacteur

Utilisez les fournisseurs MFA pour configurer l'authentification basée sur SMS et e-mail afin de garantir que chaque utilisateur peut se connecter en toute sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le ServiceNow AI Platform, vous pouvez configurer les fournisseurs de MFA avec le mécanisme d'utilisation de l'authentification multifacteur comme la messagerie et les SMS.

Vous pouvez utiliser la configuration de fournisseur suivante disponible pour la MFA dans :ServiceNow AI Platform

- Configuration du fournisseur de messagerie
- Configuration du fournisseur Twilio
- Configuration du fournisseur d'informations.

Remarque :
Twilio et la configuration du fournisseur d'informations sont renseignées automatiquement grâce à l'activation de l'option Charger les données de démonstration lors de l'installation des modules d'extension Authentification multifacteur avec SMS (com.snc.authentication.sms_mfa) et Notification - Twilio Direct Driver (com.snc.notify.twilio_direct).

Vous pouvez également créer votre propre configuration de fournisseur pour activer l'authentification multifacteur par SMS et e-mail.

Remarque :
La configuration du fournisseur d'informations est fournie dans le cadre des données de démonstration. Vous pouvez modifier les champs en fonction de vos besoins de configuration pour votre propre fournisseur.

Configurer le fournisseur MFA

Configurez les SMS et les e-mails avec le fournisseur pour vous assurer que chaque utilisateur peut se connecter en toute sécurité.

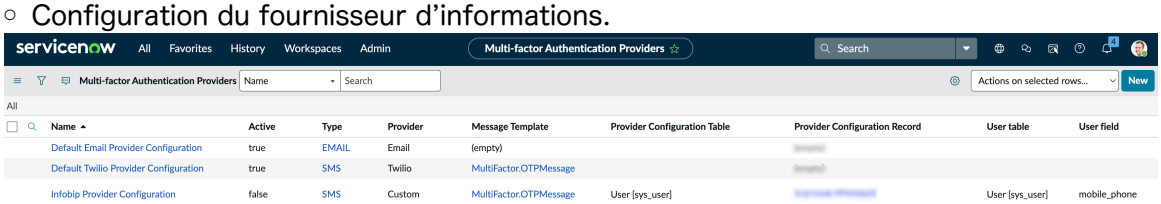
Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Fournisseurs**.

   Les configurations de fournisseur suivantes sont disponibles pour la MFA dans :ServiceNow AI Platform

   - Configuration du fournisseur de messagerie
   - Configuration du fournisseur Twilio
   - Configuration du fournisseur d'informations.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Pour créer un nouveau fournisseur, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Condition

Champ	Description
Nom	Nom de l'enregistrement.
Type	Description de l’enregistrement.
Fournisseur	Choisissez **Twilio** ou **Personnalisé**. **Remarque :** Pour configurer Twilio, consultez Configurer Notification avec Twilio. Lorsque vous choisissez **Personnalisé**, vous devez spécifier les champs suivants : ○ Table de configuration du fournisseur ○ Enregistrement de configuration du fournisseur ○ Script ○ Table des utilisateurs ○ Champ d'utilisateur
Modèle de message	Modèle de message pour l’enregistrement.
Actif	Option permettant d’activer la configuration du fournisseur.

4. Cliquez sur **Envoyer**.

En fonction du modèle de message et des configurations du fournisseur, le SMS ou l’e-mail est envoyé aux utilisateurs comme facteur d’authentification pendant le processus de connexion.

Configuration personnalisée du fournisseur Vonage (didacticiel)

Configurez un SMS avec le fournisseur Vonage pour vous assurer que chaque utilisateur peut se connecter en toute sécurité.

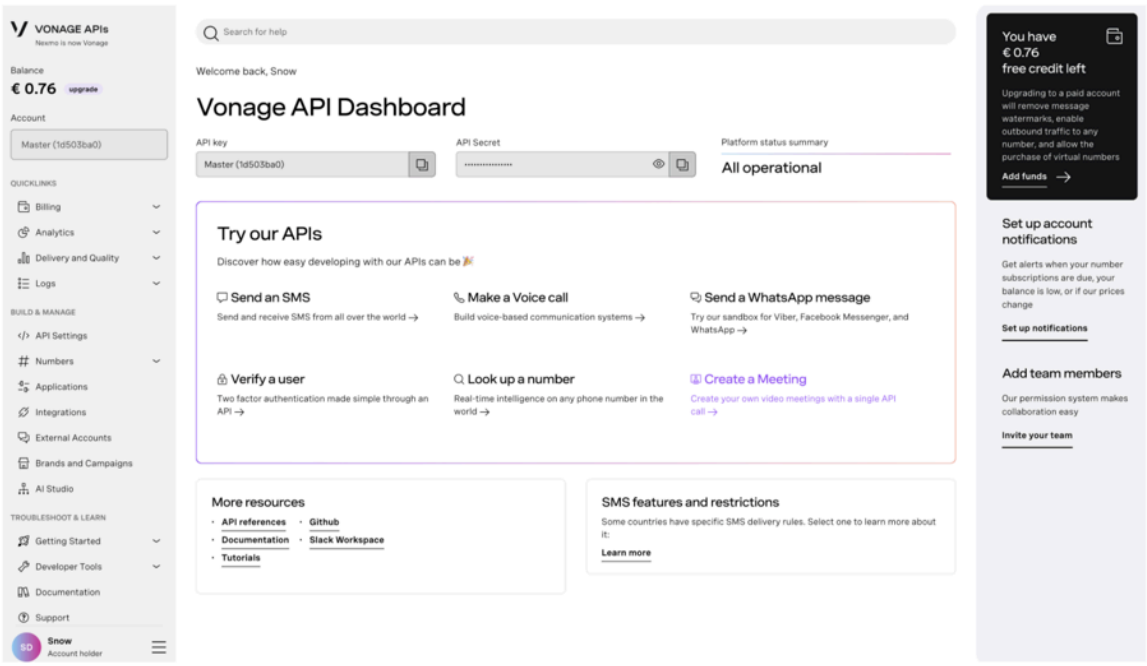
Avant de commencer
Rôle requis : admin

Traduction automatique

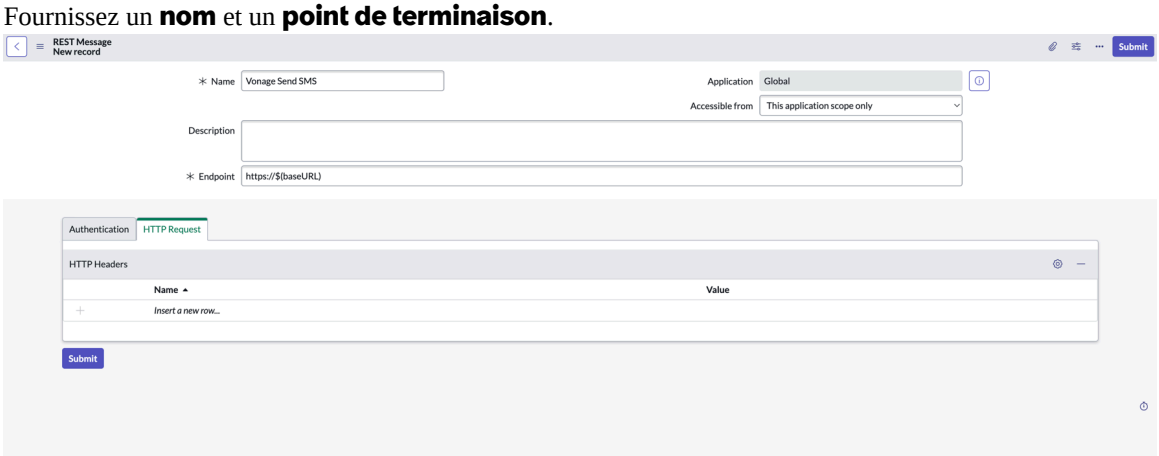
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Sortant** > **Message REST** et effectuer la configuration du message REST en fonction des informations du tableau de bord de l'API Vonage.



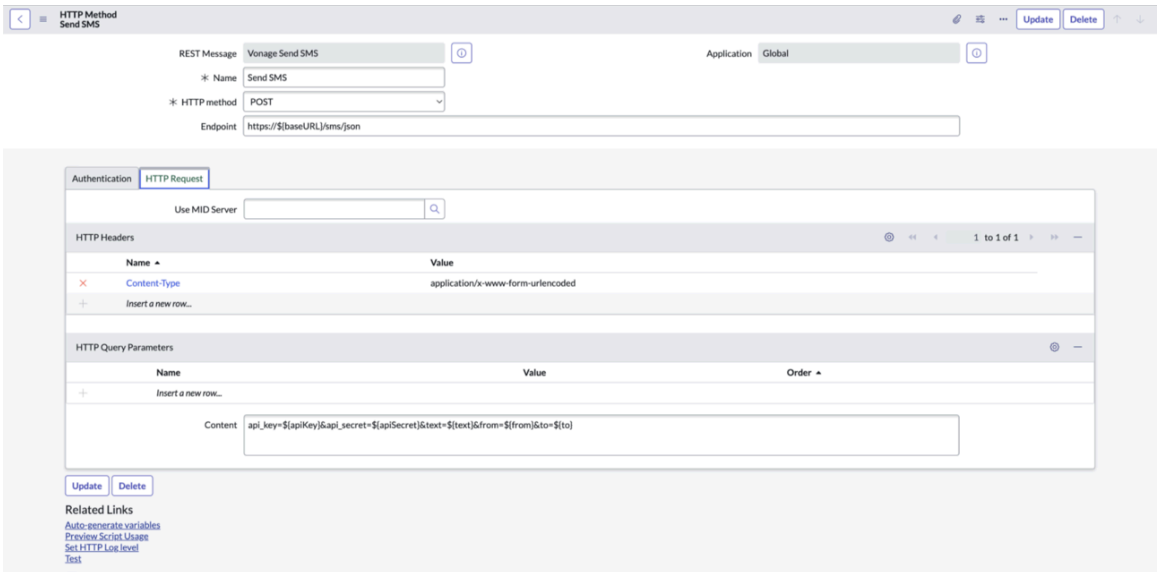
2. Cliquez sur **Nouveau** pour créer un **message REST**.
3. Fournissez un **nom** et un **point de terminaison**.



4. Cliquez sur **Envoyer**.
5. Ouvrez l'enregistrement créé, dans la liste connexe **Méthodes HTTP**, cliquez sur **Nouveau** et sélectionnez la méthode HTTP comme **POST.**
6. Renseignez les champs suivants :
   - Point de terminaison : `https://${baseURL}/sms/json`
   - Contenu :`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - Type de contenu : `application/x-www-form-urlencoded`

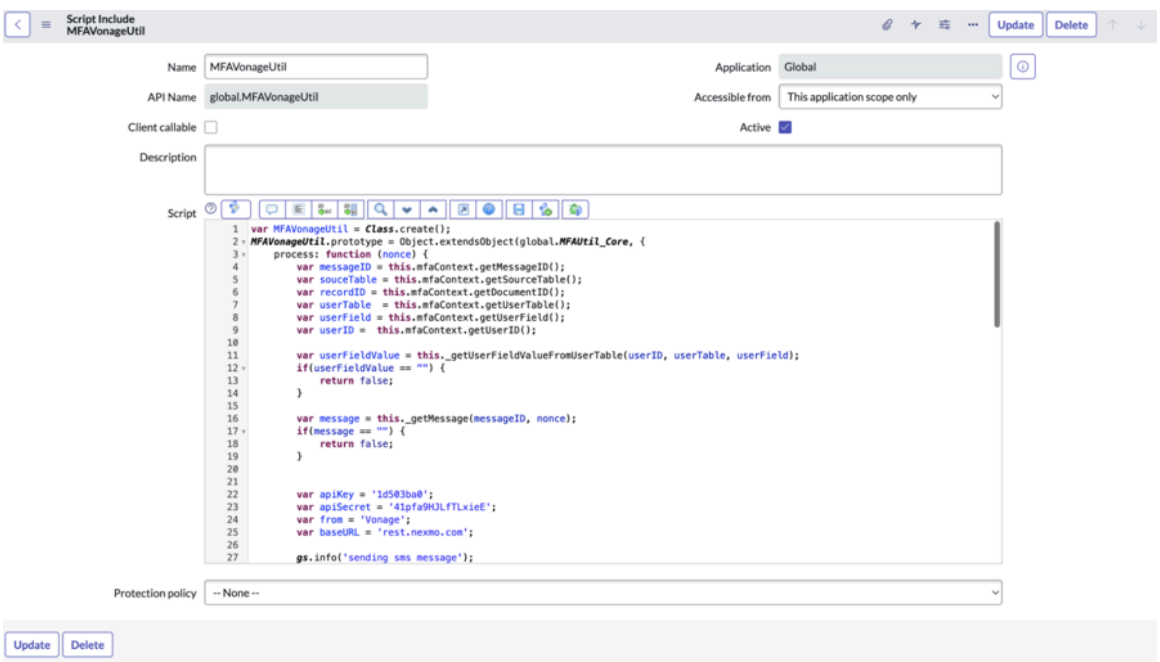
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Mettez à jour l'enregistrement
8. Cliquez sur **Générer automatiquement des variables** dans la section **Liens connexes** .
9. Importez le SI partagé dans le dossier et copiez l'apiKey et le secret à partir du tableau de bord de l'API Vonage.

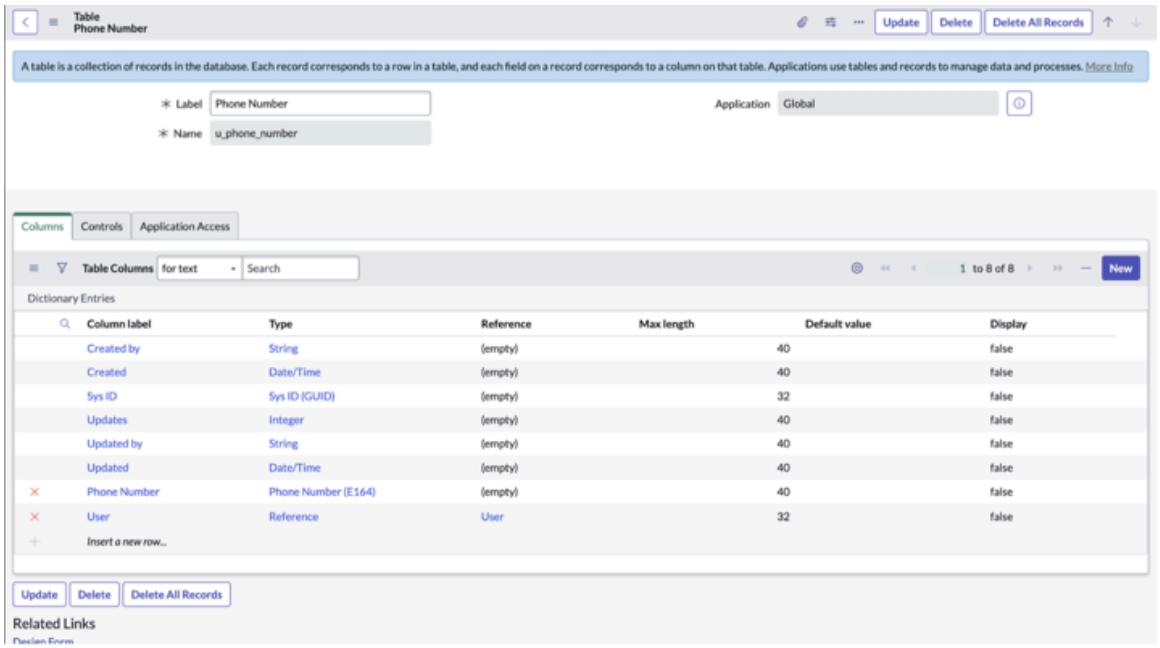
> **Remarque :**
>
> L'apiKey et le secret se trouvent dans les paramètres de votre compte Vonage dans le tableau de bord Vonage.



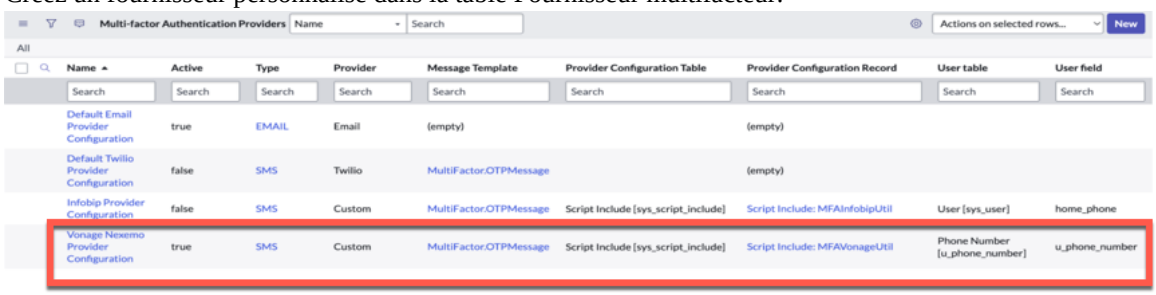
10. Créez une table personnalisée Numéros de téléphone avec deux colonnes, par exemple :
    - **Étiquette de colonne** : utilisateur, **type** : référence, **référence** : utilisateur (sys_user).
    - **Étiquette de colonne** : Numéro de téléphone, **Type** : Numéro de téléphone (E164).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Créez un fournisseur personnalisé dans la table Fournisseur multifacteur.



Pour en savoir plus sur la configuration du fournisseur, reportez-vous à la section Configurer le fournisseur MFA.

L'e-mail en tant que facteur MFA

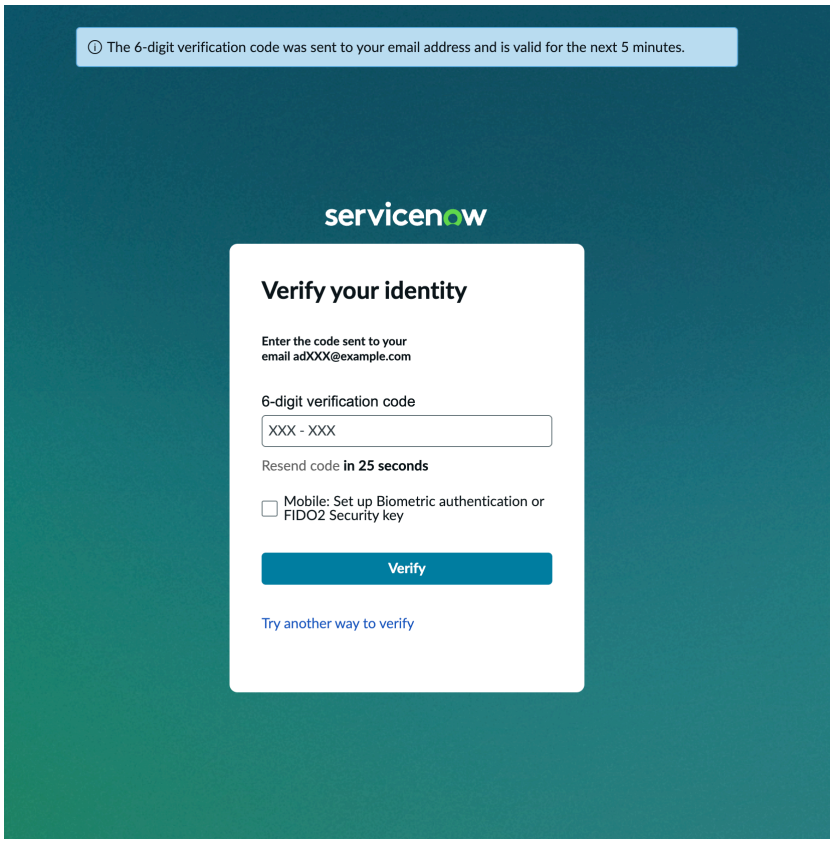
Authentification multifacteur (MFA) avec e-mail comme facteur d'authentification.

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de se connecter à l'instance à l'aide d'un OTP basé sur un e-mail.

Remarque :
MFA avec e-mail est activé par défaut avec le module d'extension Intégration - Authentification multifacteur (com.snc.integration.multifactor.authentication). Vous devez configurer les entrées et les conditions de la politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP e-mail est envoyé à l'adresse e-mail associée. L'utilisateur peut saisir le code de vérification à six chiffres qu'il a envoyé à l'adresse e-mail et confirmer son identité.

Configurer l'e-mail en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher l'OTP d'e-mail en tant que politique de facteur MFA pour l'authentification.

Avant de commencer

Rôle requis : admin

Procédure

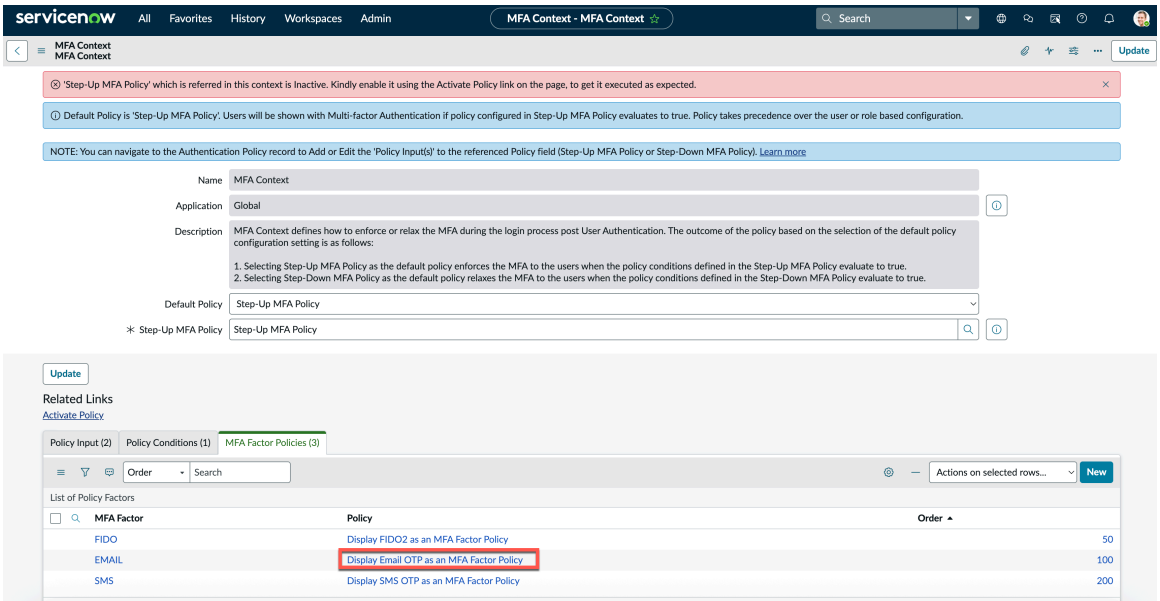
1. Accédez à la **Tous** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur **l'onglet Politiques de facteur MFA** .

> **Remarque :**
> **L'E-MAIL** en tant que **facteur MFA avec une politique** est disponible par défaut. Vous pouvez modifier la politique et spécifier ses entrées et conditions.

3. Sélectionnez Afficher **l'e-mail OTP comme politique de facteur MFA**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

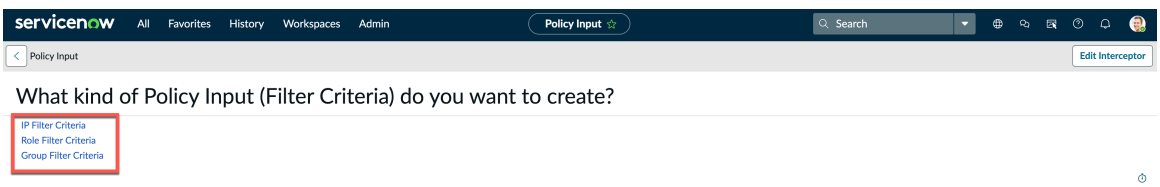


4. Cliquez sur **Nouveau** pour ajouter des **entrées de politique**.
5. Sélectionnez les critères de filtre que vous souhaitez créer.

   Les types de critères de filtre sont les suivants :

   - Critère de filtre d'adresses IP
   - Critère de filtre de rôle
   - Critère de filtre de groupe

   Par exemple, Critères de filtre de rôle.



6. Cliquez sur **Critères de filtre de rôle**, renseignez les champs correspondant aux critères de filtre de rôle et envoyez l'enregistrement.
   La nouvelle politique est créée. Pour plus d'informations, consultez Critères de filtre de rôle.
7. Sur la page Politique - Afficher le mot de passe à usage unique de l'e-mail en tant que politique de facteur MFA, cliquez sur **Conditions de la politique**.
8. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
9. Renseignez les champs suivants du formulaire :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtre) utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basés sur les rôles qui a été créée pour la condition.

10. Cliquez sur **Envoyer**.
11. **Facultatif :** Répétez l'étape 8 pour créer des conditions de politique supplémentaires.

> **Remarque :**
> Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la politique sera évaluée comme vraie si l'une de vos conditions de police est remplie.

En fonction de la politique de filtre de rôle (utilisateurs) et des conditions spécifiées pour le rôle en correspondance, le facteur MFA de courrier électronique est affiché comme une option d'authentification pour les utilisateurs.

Propriétés système de l'authentification multifacteur

Utilisez les propriétés système pour activer et personnaliser l'authentification multifacteur en fonction de vos exigences de sécurité.

Propriétés d'authentification multifacteur

Propriété	Description
`glide.authenticate.multifactor`	Activer l'authentification multifacteur.
`glide.authenticate.multifactor.setup.bypass.count`	Nombre de fois qu'un utilisateur peut choisir d'ignorer la configuration de la MFA. La valeur par défaut est 0.
`glide.multifactor.onetime.code.validity`	Nombre de minutes pendant lesquelles le code de réinitialisation est valide. Consultez Se connecter avec l'authentification multifacteur. La valeur par défaut est 5. **Remarque :** Cette propriété concerne le temps de validation OTP de l'e-mail.
`glide.authenticate.multifactor.clock_skew`	Nombre de secondes supplémentaires pendant lesquelles le code de réinitialisation est valide. Le maximum est de 60. La valeur par défaut est 10.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés d'authentification multifacteur (suite)

Propriété	Description
	L'instance valide le code saisi par l'utilisateur par rapport au code unique généré par l'application qui est généré à l'heure actuelle. Vous pouvez incliner la fenêtre temporelle avec cette propriété et permettre à un ou plusieurs codes d'être générés pendant une fenêtre temporelle pour être considérés comme valides. La valeur de la propriété est utilisée dans le calcul suivant : heure actuelle - X/2 et heure actuelle + X/2, où X est la valeur de cette propriété. Si vous utilisez la valeur de 10, par exemple, l'instance considère que tous les codes générés par l'application dans la plage horaire [l'heure actuelle - 5 secondes] et [l'heure actuelle + 5 secondes] sont valides. Utilisez cette propriété pour éviter les problèmes de connexion où l'utilisateur n'est pas en mesure de saisir le code correct dans le temps imparti par défaut.
glide.authenticate.multifactor.remember.browser.enable	Configurez cette propriété pour qu'elle invite un utilisateur à utiliser la MFA lorsqu'il se connecte à partir d'un nouvel appareil ou d'un nouveau navigateur. La valeur par défaut est oui.
glide.authenticate.multifactor.browser.fingerprint.validity	Une fois que l'authentification multifacteur mémorise le navigateur, l'utilisateur n'est pas mis en service pour l'authentification multifacteur dans le même navigateur pendant cette durée. La valeur par défaut est de 8 heures.
glide.authenticate.multifactor.remember.browser.max.count	Nombre de navigateurs dont la MFA se souvient pour cet utilisateur.
glide.authenticate.multifactor.remember.default	Valeur par défaut de la case à cocher remember-browser dans la page multifacteur de validation.
glide.webauthn.enabled)	Option permettant d'activer les méthodes d'authentification sans mot de passe (MFA basée sur FIDO2) telles que la clé matérielle et l'authentification biométrique.
glide.authenticate.multifactor.email.otp.enable	Option permettant d'activer l'OTP basé sur l'e-mail en tant que facteur pour la MFA.
glide.auth.mfa.ui.v2.enabled	Option permettant d'activer le facteur MFA indépendamment pour les utilisateurs sans configurer d'application d'authentification.

Critères d'authentification multifacteur

Utilisez les critères MFA pour déterminer quels utilisateurs et rôles doivent utiliser la vérification en deux étapes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critère multifacteur

Utilisez les critères MFA pour déterminer quels utilisateurs et rôles doivent utiliser la vérification en deux étapes. Vous pouvez utiliser l'un de ces critères ou une combinaison de ceux-ci en fonction des besoins de votre entreprise. Vous pouvez utiliser l'un de ces critères ou une combinaison de ceux-ci en fonction des besoins de votre entreprise.

Remarque :
Il est recommandé d'utiliser l'authentification MFA basée sur la politique d'authentification adaptative.

Critère multifacteur basé sur l'utilisateur

Utilisez des critères multifacteur basés sur l'utilisateur pour sélectionner les utilisateurs individuels qui doivent se connecter à l'aide de la MFA. Les administrateurs mettent à jour le champ **Activer l'authentification multifacteur** sur un enregistrement utilisateur pour activer ou désactiver les exigences MFA pour un utilisateur. Pour obtenir des détails sur ce processus, consultez Configurer les critères multifacteur basés sur l'utilisateur.

Critère multifacteur basé sur le rôle

Utilisez des critères multifacteur basés sur les rôles pour exiger une connexion MFA pour tous les utilisateurs affectés à un rôle spécifique. L'enregistrement **d'authentification multifacteur basée sur les rôles** de la table **Critères multifacteur** [multi_factor_criteria] contient la liste des rôles qui nécessitent une connexion MFA. Pour plus d'informations sur la gestion de cette liste, reportez-vous à la section Configurer les critères multifacteur basés sur les rôles.

Critères multifacteur basés sur une politique d'authentification adaptative

Utilisez l'authentification adaptative pour déterminer quand votre instance nécessite l'authentification MFA. L'authentification adaptative utilise des politiques d'authentification pour évaluer des critères tels que l'adresse IP d'un utilisateur ou des groupes d'utilisateurs. Pour plus d'informations sur la fonction d'authentification adaptative, reportez-vous à la section Authentification adaptative.

Configurer les critères multifacteur basés sur l'utilisateur

Utilisez des critères multifacteur basés sur l'utilisateur pour activer la MFA pour un utilisateur.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.
2. Configurez la liste pour afficher la colonne **Activer l'authentification multifacteur** .
3. Changez les valeurs de la colonne **Activer l'authentification multifacteur** pour les utilisateurs sélectionnés sur **vrai**.

   Lorsque l'utilisateur se connecte avec son nom d'utilisateur et son mot de passe, il est invité à configurer l'authentification multifacteur.

Configurer les critères multifacteur basés sur les rôles

Utilisez des critères multifacteur basés sur les rôles pour appliquer l'authentification multifacteur à tous les utilisateurs affectés à des rôles spécifiques.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Critère multifacteur**.
2. Dans la liste **Critères multifacteur** , ouvrez l'enregistrement **Authentification multifacteur basée sur les rôles** .
3. Utilisez la liste **Rôles multifacteur** pour ajouter ou supprimer des rôles.

Option	Description
Ajouter un rôle	Double-cliquez sur **Insérer une nouvelle ligne...** et entrez ou sélectionnez un nom de rôle. Cliquez sur **l'icône Enregistrer** ( ) pour enregistrer l'entrée.
Supprimer un rôle	Cliquez sur l'icône de suppression (icône de) pour supprimer un rôle de la liste.

4. Cliquez sur **Mettre à jour**.

Résultats

Votre instance applique l'authentification multifacteur pour tous les utilisateurs qui sont membres des rôles répertoriés dans la liste **Rôles multifacteur** .

Important :
L'enregistrement doit être actif pour appliquer l'authentification multifacteur basée sur les rôles.

Configurer les critères multifacteur basés sur une politique d'authentification adaptative

Utilisez des politiques adaptatives pour déterminer quels utilisateurs doivent utiliser la vérification multifacteur (MFA) en deux étapes.

Avant de commencer

Rôle requis : admin

Remarque :

- Si la politique par défaut est **une politique MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans **la politique MFA** ascendante est évaluée comme vraie. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.
- MFA avec connexion SSO n'est disponible que si la propriété glide.authenticate.mfa.with.multisso.enabled est définie sur vrai.
- Vous pouvez accéder à l'enregistrement Politique d'authentification pour ajouter ou modifier les « entrées de la politique » au champ de politique référencé (**Politique de MFA ascendante** ou **Politique de MFA descendante**).

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte MFA**.
   L'enregistrement de contexte de politique **MFA** s'ouvre.
2. Sélectionnez la politique par défaut dans le champ **Politique par défaut** .
   Cette sélection détermine la façon dont votre instance utilise les conditions de politique pour déterminer si elle doit exiger l'authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques par défaut

Politique par défaut	Définition
Politique MFA ascendante	Sélectionnez cette option pour appliquer la MFA lorsque les conditions de politique définies dans la **politique de MFA ascendante** sont évaluées comme vraies.
Politique MFA descendante	Sélectionnez cette option pour contourner la MFA lorsque les conditions de politique définies dans la **politique MFA descendante** sont évaluées comme vraies.

3. Dans le champ **Politique de MFA** ascendante, sélectionnez une politique à utiliser avec ce contexte.
4. Cliquez sur **Mettre à jour**.
   Après avoir sauvegardé l'enregistrement, les listes **Entrée de politique** et **Conditions de politique** se mettent à jour pour afficher les entrées de politique et les conditions associées à la politique sélectionnée dans le champ **Politique de MFA** ascendante.

Authentification multifacteur avec authentification unique

Vous pouvez utiliser la MFA avec un fournisseur SSO pour votre ServiceNow instance.

Étant donné que de nombreux utilisateurs de votre organisation se connectent à votre réseau d'entreprise et accèdent à votre ServiceNow instance, il existe un besoin accru d'authentification sécurisée.

La MFA avec la combinaison de SSO fournit une sécurité renforcée pour votre instance. Cette fonctionnalité offre la flexibilité nécessaire pour activer l'authentification multifacteur sous conditions pour les utilisateurs.

Remarque :

- ServiceNow L'authentification multifacteur est appliquée une fois que l'utilisateur est redirigé après l'authentification réussie auprès du fournisseur d'identité.
- La MFA n'était pas appliquée avec SSO avant la version San Diego.

Par exemple, si vous souhaitez donner à vos utilisateurs externes un protocole de sécurité supplémentaire, vous pouvez appliquer la MFA à ces utilisateurs uniquement. De cette façon, vous pouvez ajouter des capacités d'authentification supplémentaires et contrôler l'accès de vos utilisateurs.

Pour les connexions basées sur SSO telles que SAML, OpenID Connect et Digest, vous pouvez appliquer la MFA pour l'authentification.

La MFA avec SSO peut être configurée sur demande en fonction de vos besoins. À l'aide de schémas d'authentification et de fournisseurs d'identité, vous pouvez appliquer la MFA pour des utilisateurs spécifiques avec un mécanisme de connexion spécifique.

Vous pouvez appliquer la MFA pour les conditions suivantes :

- Schéma d'authentification
- Fournisseur d'identité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La MFA avec SSO est proposée dans le cadre du module d'extension Authentification adaptative (com.snc.adaptive_authentication). Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à la section Authentification adaptative.

Configuration de la MFA avec SSO

Appliquez la MFA avec SSO pour vos utilisateurs au sein ou en dehors de votre organisation.

Avant de commencer

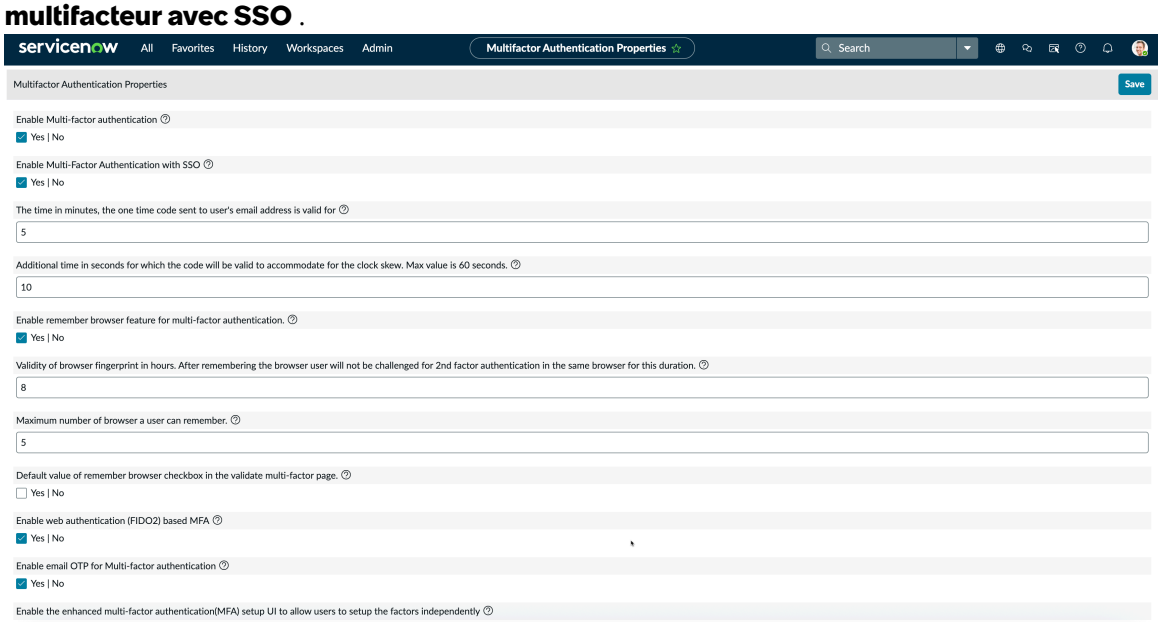
La fonctionnalité MFA avec SSO est proposée dans le cadre du module d'extension Authentification adaptative (com.snc.adaptive_authentication). Vous devez activer la propriété d'authentification adaptative pour utiliser la MFA avec la fonctionnalité SSO. Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à la section Authentification adaptative.

Remarque :
La MFA avec connexion SSO est disponible si la `glide.authenticate.mfa.with.multisso.enabled` propriété est définie sur **vrai**.

Rôle requis : admin

Procédure

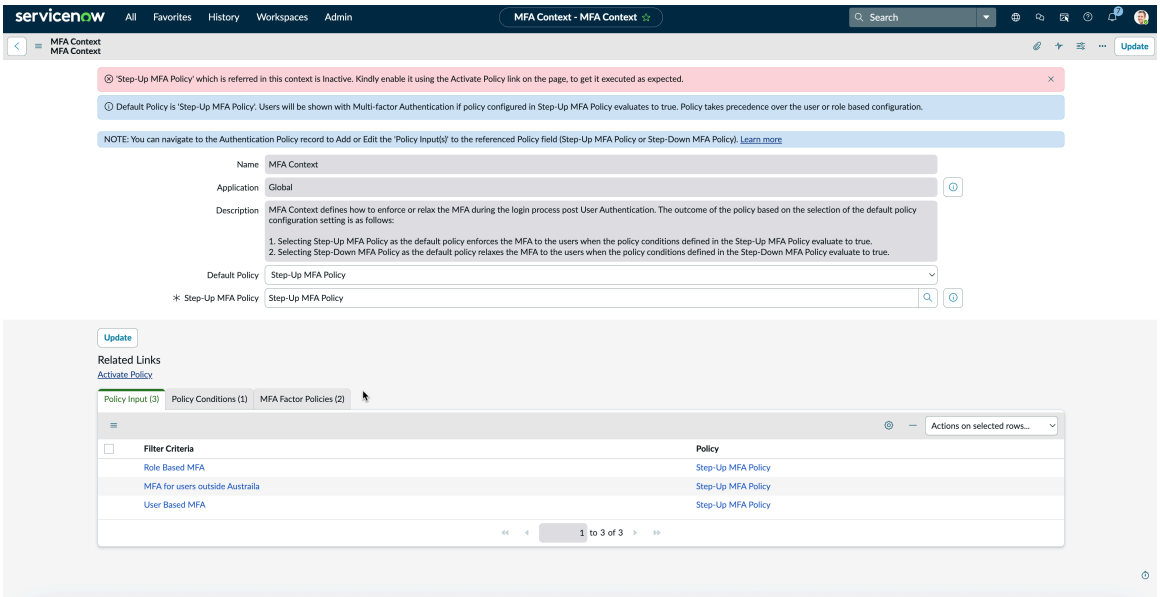
1. Accédez à la **Tous** > **Authentification multifacteur** > **Propriétés**.
2. Cochez les cases **Activer l'authentification multifacteur** et **Activer l'authentification multifacteur avec SSO** .



3. Cliquez sur **Enregistrer**.
4. Accédez à la **Authentification multifacteur** > **Contexte MFA**.
   Le formulaire Contexte MFA s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Par défaut, il s'agit **d'une politique MFA ascendante**. Les utilisateurs s'affichent avec l'authentification multifacteur si une condition configurée dans **la politique de configuration MFA** donne la valeur **vrai**. La politique a priorité sur la configuration basée sur l'utilisateur ou les rôles.

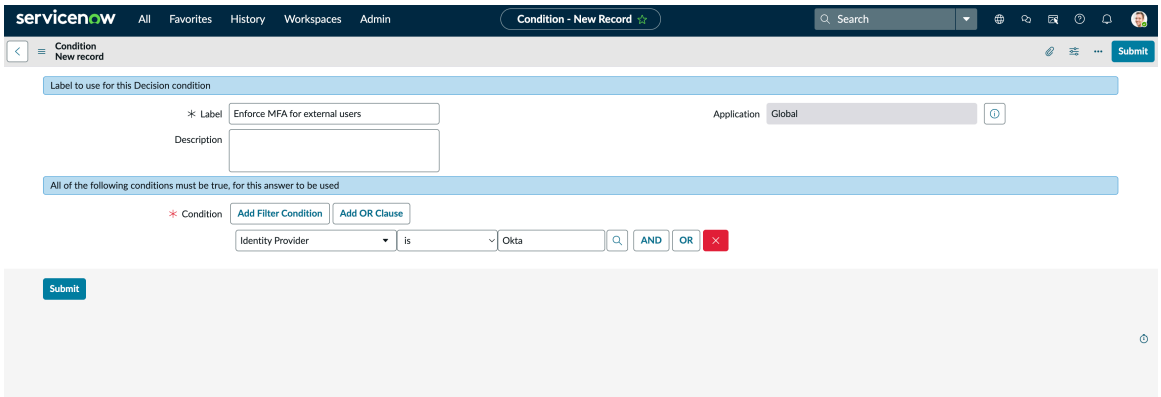
5. **Facultatif :** Pour modifier une politique, revenez à l'enregistrement de la politique d'authentification, modifiez les conditions et revenez.
   Lorsque vous accédez à l'enregistrement de la politique d'authentification, vous pouvez ajouter ou modifier les « entrées de la politique » aux champs de politique référencés, **Politique de MFA** ascendante ou **Politique de MFA descendante**.
6. Pour définir une nouvelle condition de politique, cliquez sur **Conditions de la politique**.
7. Cliquez sur **Nouveau**.
8. Remplissez les champs du formulaire.

Formulaire Conditions

Champs	Description
Étiquette	Nom unique de la condition que vous souhaitez créer pour l'étiquette.
Description	Description de la condition de politique.
Conditions	Le type de condition que vous souhaitez appliquer pour la police. Vous pouvez ajouter des conditions de filtre et des clauses « OU ». **Remarque :** L'ajout de diverses conditions et clauses de filtre vous permet de contester l'authentification multifacteur pour des utilisateurs spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Example

Pour configurer vos conditions, considérez l'exemple suivant. Supposons que vous souhaitiez que le schéma d'authentification avec le fournisseur d'identité soit votre condition pour les utilisateurs externes. Vous pouvez définir les conditions comme suit :

a. Sélectionnez **Schéma d'authentification** et définissez les critères comme **Authentification unique** ou **Nom d'utilisateur et mot de passe**.

En fonction de cette sélection, l'utilisateur reçoit une connexion basée sur SSO ou un formulaire de connexion pour spécifier le nom d'utilisateur et le mot de passe.

b. Sélectionnez **Fournisseur d'identité** et indiquez le fournisseur comme enregistrement IdP pour lequel vous souhaitez activer la MFA. Par exemple, **Okta**.

Sur la base de cette sélection, si l'utilisateur se connecte avec le SSO, il n'a pas de problème avec la MFA. En revanche, si l'utilisateur se connecte à l'aide Okta de , il est confronté à l'authentification multifacteur.

9. Cliquez sur **Envoyer**.

Information associée

Authentification adaptative

Authentification multifacteur avec authentification unique

Réinitialiser l'authentification multifacteur (MFA) pour les utilisateurs

Les administrateurs peuvent réinitialiser l'authentification multifacteur pour les utilisateurs qui ont supprimé l'application, perdu l'accès à l'appareil ou qui n'ont pas d'autre authentification multifacteur associée à leur appareil.

Avant de commencer

Rôle requis : admin

La procédure suivante décrit comment un ServiceNow® administrateur peut réinitialiser la validation MFA pour débloquer des utilisateurs et leur permettre de réenregistrer MFA.

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.

2. Recherchez l'utilisateur que vous souhaitez débloquer.

3. Définissez la valeur Valider sur **faux**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Accédez à la **Tous** > **Authentification multifacteur** > **Authentification Web** > **Informations d'identification publiques de l'utilisateur (sys_user_public_credential**.
5. Recherchez l'utilisateur que vous souhaitez débloquer.
6. Supprimez tous les enregistrements pour cet utilisateur.
7. Accédez à la **Tous** > **Authentification multifacteur** > **Facteurs de l'utilisateur récent de l'utilisateur**.
8. Recherchez le même utilisateur.
9. Supprimez tous les enregistrements pour cet utilisateur.

Résultats

Lorsque l'utilisateur débloqué saisit les informations d'identification et se connecte, la page **Activer l'authentification multifacteur (MFA)** s'affiche. L'utilisateur peut suivre les étapes de la page pour réenregistrer l'authentification multifacteur.

Rubrique de référence - Authentification multifacteur

Rubrique de référence relative à la configuration de l'authentification multifacteur.

Authentifications multifacteurs pour les utilisateurs

Pour accéder aux détails de la MFA de l'utilisateur, accédez à **Tous** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.

Authentifications multifacteurs pour les utilisateurs

Champ	Description
Utilisateur	Le nom d'utilisateur de l'utilisateur
Contournements restants	Nombre total de contournements qui restent pour l'utilisateur.
Secret multifacteur	Les détails du secret multifacteur.
Validés	Le multifacteur est-il validé ? Changer la valeur en **faux** invalide la configuration d'application d'authentification existante.

Remarque :
Les facteurs MFA récemment utilisés par les utilisateurs sont disponibles dans le module Facteurs utilisateur utilisés récemment. Accédez à la **Tous** > **Authentification multifacteur** > **Facteurs de l'utilisateur récent de l'utilisateur**. Pour plus d'informations, consultez Facteurs de l'utilisateur utilisés récemment.

Empreintes digitales du navigateur multifacteur

Pour accéder aux détails des empreintes digitales du navigateur de l'utilisateur, accédez à **Tous** > **Authentification multifacteur** > **Empreintes digitales du navigateur multifacteur**.

Empreintes digitales du navigateur multifacteur

Champ	Description
Utilisateur	Le nom d'utilisateur de l'utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Empreintes digitales du navigateur multifacteur (suite)

Champ	Description
Navigateur	Le navigateur que l'utilisateur a utilisé.
Empreinte digitale du navigateur	Détails des empreintes digitales du navigateur.
Cookie d'empreinte digitale du navigateur	Détails du cookie d'empreinte digitale du navigateur.
Expiration du cookie d'empreinte digitale du navigateur	Détails d'expiration du cookie d'empreinte digitale du navigateur.

Facteurs de l'utilisateur utilisés récemment

Pour accéder aux détails des facteurs que l'utilisateur a récemment utilisés, accédez à **Tous** > **Authentification multifacteur** > **Facteurs de l'utilisateur récent de l'utilisateur**.

Configurations multifacteurs pour les utilisateurs

Champ	Description
Utilisateur	Le nom d'utilisateur de l'utilisateur
Type multifacteur	Le type multifacteur que l'utilisateur a utilisé pour se connecter.
Est un facteur récent	Les détails multifacteurs récents de l'utilisateur.

Mesures MFA

Affichez les différentes mesures MFA pour comprendre l'adoption et l'utilisation de la MFA.

Les mesures liées à la MFA sont disponibles dans le Centre de sécurité. Security Center est une application gratuite que vous pouvez télécharger depuis le ServiceNow Store. Pour plus d'informations sur le Centre de sécurité, reportez-vous à la section Page de destination de Centre de sécurité.

Dans Centre de sécurité, utilisez la barre en haut de la page pour naviguer entre les sections de la console de surveillance de sécurité et sélectionnez l'onglet **Mesures de sécurité** .

Les mesures MFA sont les suivantes :

- Utilisateurs inscrits pour la MFA : nombre total d'utilisateurs inscrits pour utiliser la MFA.
- Utilisateurs utilisant le contournement MFA : nombre total d'utilisateurs qui contournent l'authentification multifacteur.
- Utilisateurs non MFA aux privilèges élevés : nombre total d'utilisateurs aux privilèges élevés qui n'utilisent pas la MFA.
- Utilisateurs de MFA actifs : nombre total d'utilisateurs de MFA actifs sur votre instance.
- Utilisateurs MFA bloqués : nombre total d'utilisateurs MFA qui sont verrouillés sur votre instance.
- Connexions locales non protégées par MFA : utilisateurs qui se sont connectés sans MFA.

Pour plus d'informations sur les mesures de sécurité, reportez-vous à la section Mesures de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de l’authentification multifacteur

Découvrez comment utiliser des outils d’authentification multifacteur pour accéder en toute sécurité à votre instance.

Se connecter avec l'authentification MFA

ServiceNow requiert des applications d'authentification qui prennent en charge les mots de passe à usage unique et durée définie (TOTP). ServiceNow teste l'authentification MFA avec les applications d'authentification suivantes :

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

Remarque :

- d'autres applications d'authentification non répertoriées peuvent également être compatibles, mais ne sont pas testées par ServiceNow.
- pour en savoir plus sur le changement de comportement spécifique du navigateur, consultez cet article de la base de connaissances .

Enregistrer une application d’authentification

Application d'authentification Vous pouvez utiliser des applications d’authentification pour utiliser un deuxième facteur d’authentification.	Si votre administrateur a activé l'authentification multifacteur (MFA) sur votre instance, vous êtes invité à effectuer une seconde authentification après avoir saisi votre nom d'utilisateur et votre mot de passe. Pour plus d’informations sur le processus de connexion MFA, reportez-vous à la section Se connecter avec l’authentification multifacteur.
Validation avec l’application d’authentification Saisissez le code affiché sur votre application d'authentification pour vous connecter.	Si vous n'avez pas configuré un second formulaire d'authentification, une page de configuration s'affiche après la connexion pour vous guider dans le processus de configuration d'une application d'authentification. Pour en savoir plus sur cette configuration, consultez Configurer l’authentification multifacteur pour la première fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Enregistrer un appareil d'authentification

Une fois que vous avez configuré une application d'authentification, vous pouvez enregistrer d'autres méthodes d'authentification.



Authentificateurs biométriques

Vous pouvez utiliser des authentificateurs biométriques comme les empreintes digitales ou la reconnaissance faciale comme seconde authentification MFA. Si votre administrateur autorise cette option, vous pouvez configurer des authentificateurs biométriques en suivant les étapes de la rubrique Enregistrer un authentificateur biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentificateurs de clé matérielle

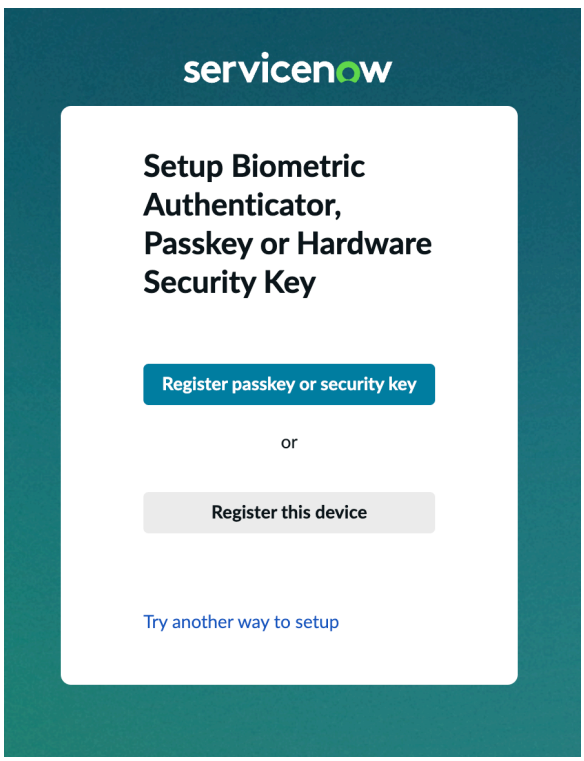
Les clés matérielles sont des appareils de sécurité physique que vous pouvez utiliser pour l'authentification. Vous pouvez enregistrer un appareil matériel à utiliser avec votre instance en suivant les étapes de la rubrique Enregistrer une clé de sécurité matérielle.



Validation avec biométrie ou clé matérielle

Utilisez la clé biométrique ou matérielle pour vous connecter.

Utilisez la biométrie ou une clé de sécurité pour vous connecter.



Traduction automatique

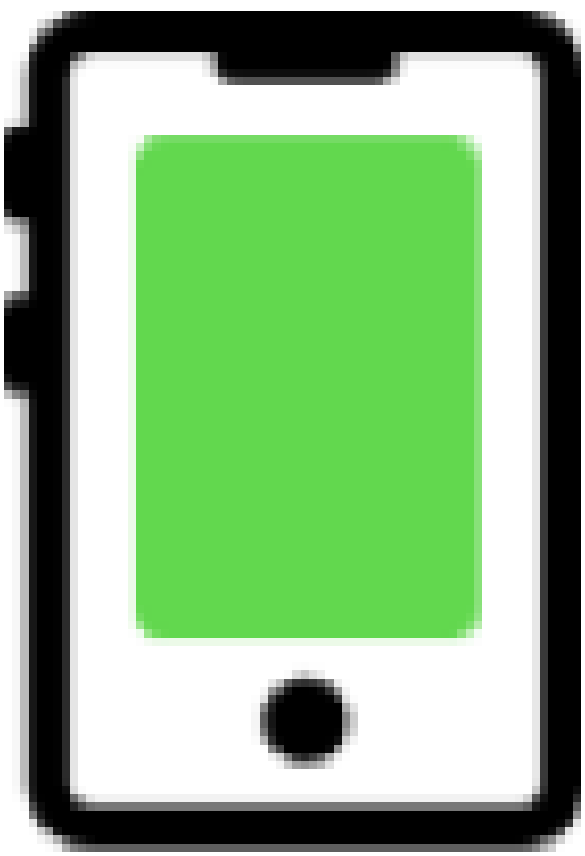
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer un numéro de téléphone pour le mot de passe à usage unique

SMS

Utilisez un OTP basé sur SMS pour exiger les utilisateurs qui tentent de se connecter.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par SMS est envoyé au numéro de téléphone mobile associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.



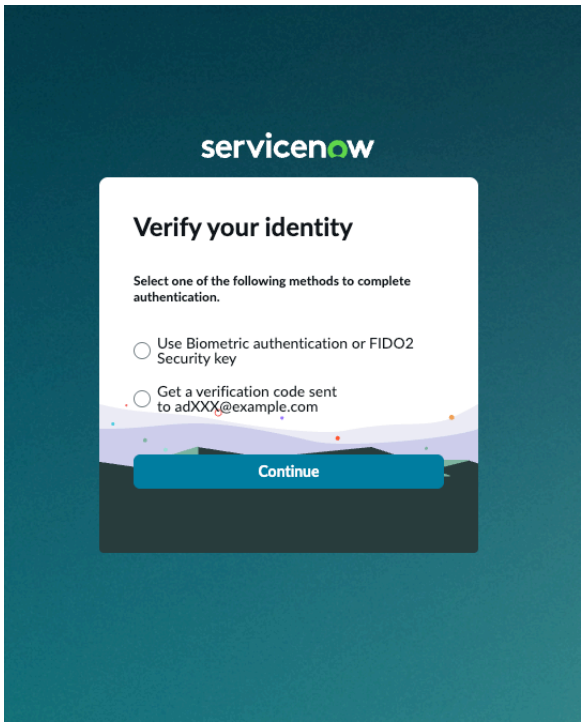
Validation par SMS

Utilisez la validation par SMS pour vous connecter en fonction de l’OTP généré.

Saisissez le code à 6 chiffres envoyé au numéro de téléphone mobile pour vous connecter. Le code envoyé est valide pendant les 5 minutes qui suivent sa réception. Vous pouvez utiliser Renvoyer le code pour que le code vous soit de nouveau envoyé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Enregistrer une adresse e-mail pour le mot de passe à usage unique

Adresse e-mail

Utilisez un OTP basé sur l’e-mail pour exiger des utilisateurs qui tentent de se connecter.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par e-mail est envoyé à l'adresse e-mail associée à l'utilisateur. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.



Validation par e-mail

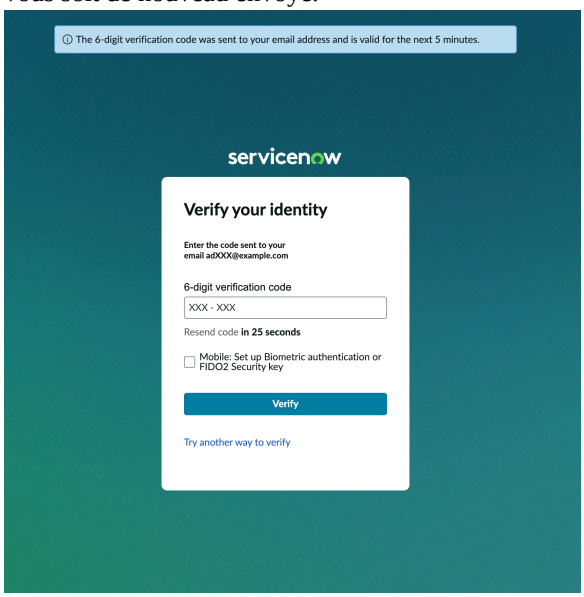
Saisissez le code à 6 chiffres envoyé à l'adresse e-mail pour vous connecter. Le code envoyé est valide

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la validation avec e-mail pour vous connecter en fonction de l'OTP généré.

pendant les 5 minutes qui suivent sa réception. Vous pouvez utiliser Renvoyer le code pour que le code vous soit de nouveau envoyé.



Configurer l'authentification multifacteur pour la première fois

Si votre administrateur a activé l'authentification multifacteur sur votre profil, mais que vous n'avez pas encore configuré l'application, vous pouvez la configurer lors de la connexion.

Avant de commencer

Rôle requis : aucun

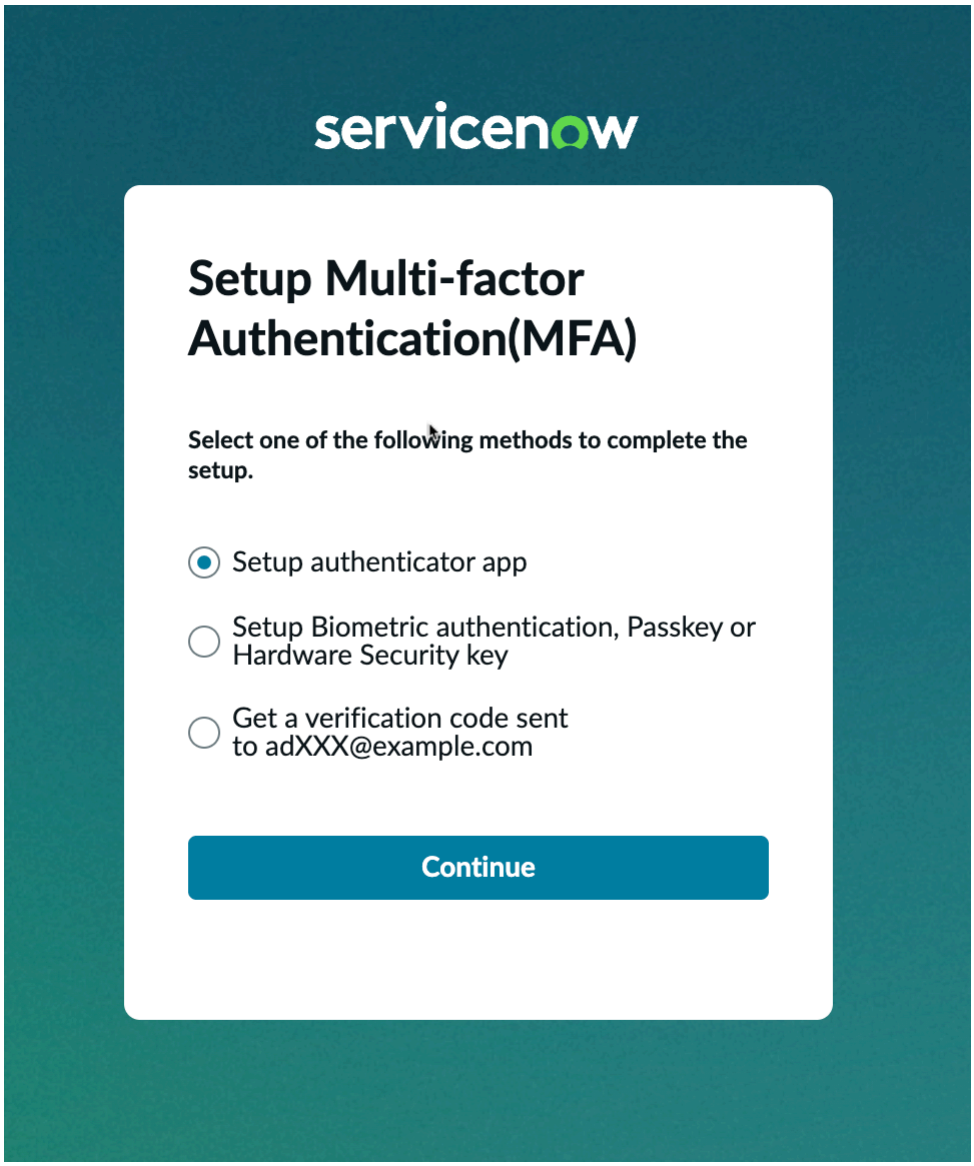
Procédure

1. Connectez-vous à votre instance à l'aide de votre nom d'utilisateur et de votre mot de passe.

L'écran de configuration de l'authentification multifacteur intercepte votre connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Si vous souhaitez ignorer la configuration de l'authentification maintenant, cliquez sur **Contournement** de la configuration. Vous pouvez contourner l'authentification multifacteur pour un nombre limité de fois que votre administrateur l'autorise. Vous devez éventuellement configurer l'authentification multifacteur.

2. Sélectionnez l'une des méthodes suivantes pour terminer la configuration de la MFA.

a. Configurer une application d'authentificateur

Suivez les instructions à l'écran pour coupler l'appareil et vous connecter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

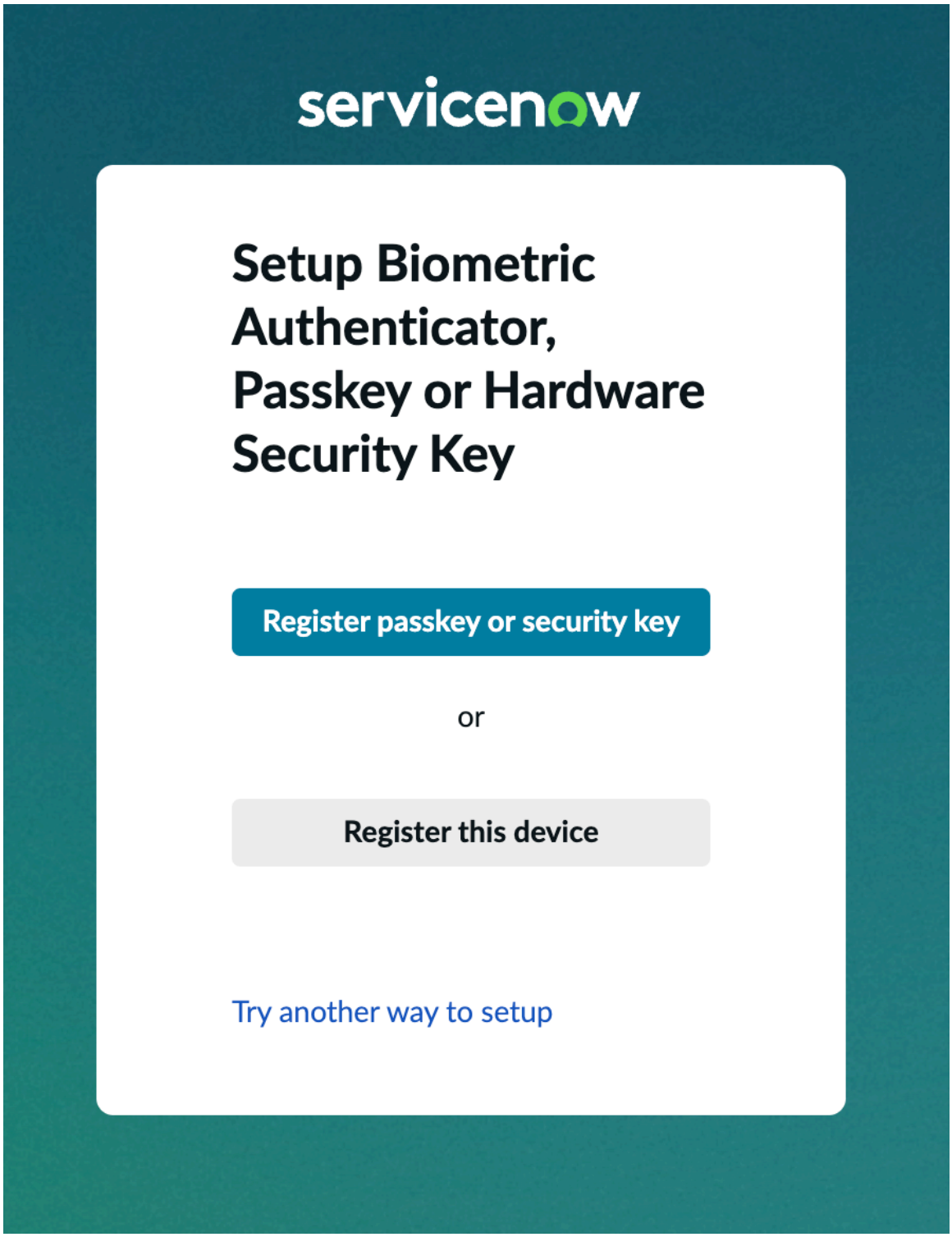


Traduction automatique

b. Configurer l'authentification biométrique, la clé d'accès ou la clé de sécurité du matériel

Sélectionnez l'une des options pour terminer la configuration.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

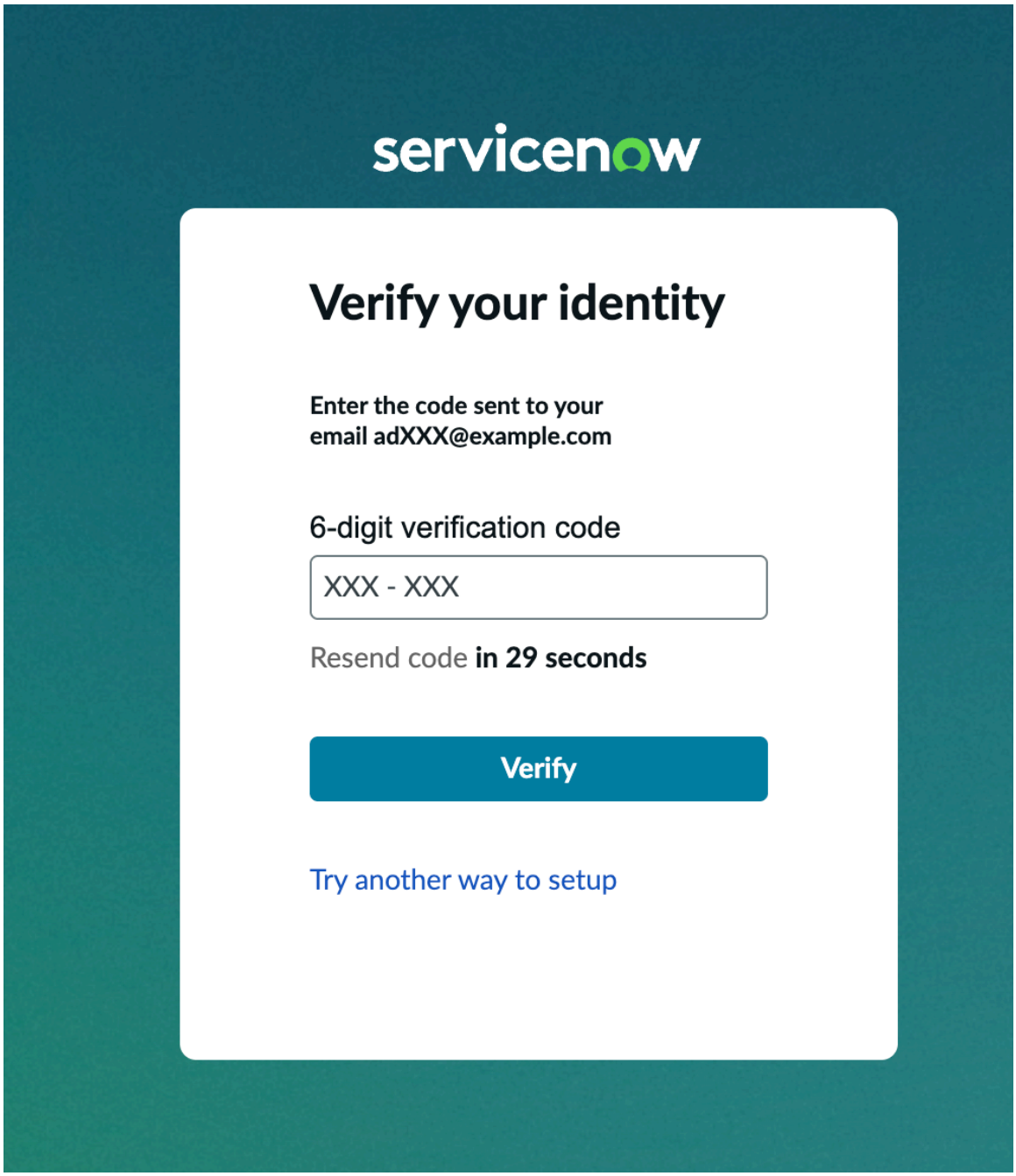


Traduction automatique

c. Recevoir un code de vérification envoyé à votre adresse e-mail

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Entrez le code de vérification qui vous est envoyé par e-mail.



Une fois que l’une ou l’autre des configurations a été terminée, vous êtes connecté à l’instance.

Configurer l’authentification multifacteur sur votre profil d’utilisateur

Activez l’authentification multifacteur pour votre compte dans les paramètres de votre profil d’utilisateur.

Avant de commencer
Rôle requis : aucun

L’authentification multifacteur doit être activée sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Votre administrateur peut vous demander d'utiliser l'authentification multifacteur. Dans ce cas, vous êtes automatiquement invité lorsque vous vous connectez. Consultez Configurer l'authentification multifacteur pour la première fois. Suivez le processus ci-dessous si votre administrateur vous autorise à accepter l'authentification multifacteur.

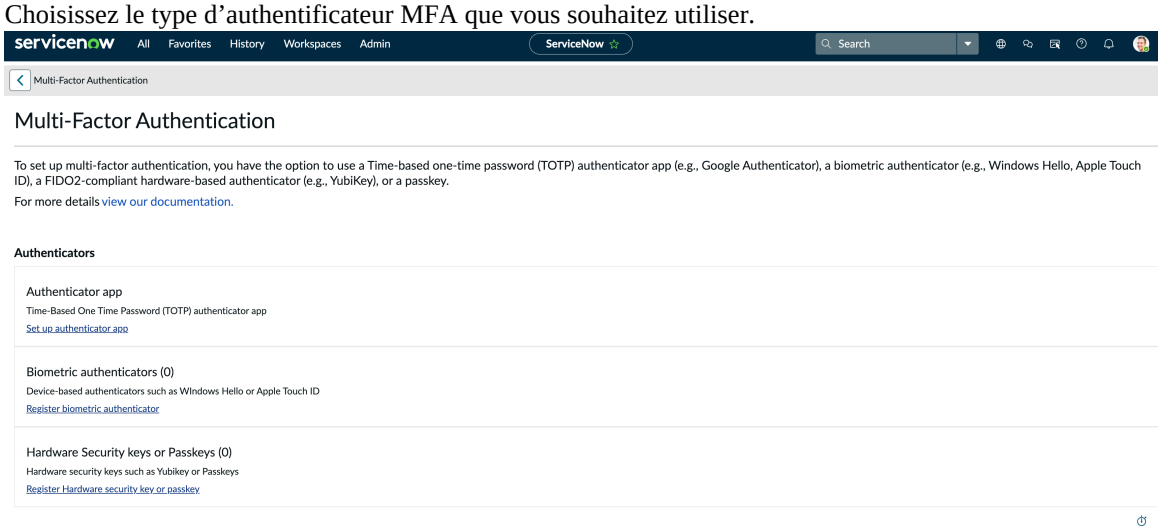
Procédure

1. Accédez à la **Tous** > **Libre-service** > **Mon profil**.

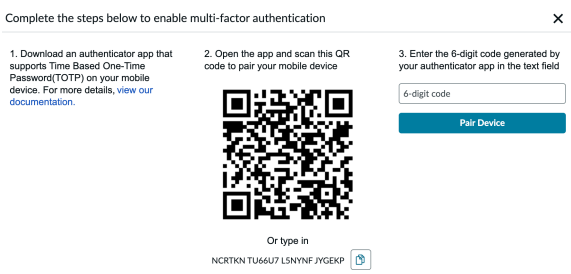
   Remarque :
   Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

2. Dans votre profil d'utilisateur, cliquez sur **Configurer l'authentification multifacteur** dans la section **Liens connexes** .

3. Choisissez le type d'authentificateur MFA que vous souhaitez utiliser.

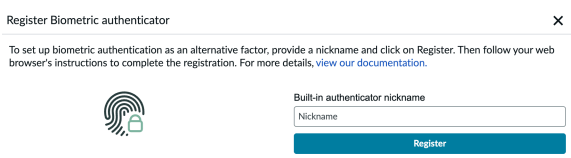
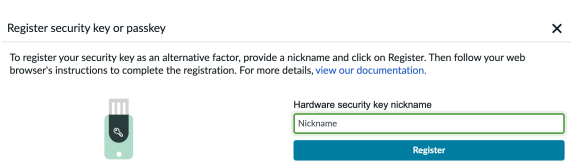


Authentificateurs MFA

Authentificateurs MFA	Description
Application d'authentification	Application d'authentification basée sur un mot de passe unique et durée définie (TOTP) Sélectionnez **Configurer une application d'authentification** et suivez les instructions à l'écran pour vous inscrire à une application d'authentification comme deuxième facteur d'authentification. 

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentificateurs MFA	Description
Authentificateurs biométriques	Authentificateurs basés sur l’appareil tels que Windows Hello ou Apple Touch ID Sélectionnez **Enregistrer l’authentification biométrique** et suivez les instructions à l’écran pour vous inscrire à une application d’authentification comme deuxième facteur d’authentification. 
Clés de sécurité matérielles	Clés de sécurité matérielles telles que YubiKey Sélectionnez **Enregistrer les clés de sécurité matérielles** et suivez les instructions à l’écran pour vous inscrire à une application d’authentification comme deuxième facteur d’authentification. 

Résultats

L’authentification multifacteur est activée pour votre compte utilisateur. Vous serez invité à utiliser l’authentification multifacteur lors de votre prochaine connexion.

Remarque :
Vous ne pouvez pas désactiver l’authentification multifacteur sur votre compte une fois que vous l’avez activée. Si vous devez désactiver l’authentification multifacteur, contactez votre administrateur.

Se connecter avec l’authentification multifacteur

Connectez-vous à l’authentification MFA lorsque son activation sera effectuée par votre administrateur sur votre instance.

Avant de commencer

Vous devez avoir activé l’authentification multifacteur pour votre profil. Vous pouvez l’activer vous-même sur votre profil d’utilisateur ou votre administrateur peut l’activer pour vous.

Rôle requis : aucun

Remarque :
Le dernier facteur de vérification MFA utilisé est automatiquement affiché pour les utilisateurs lors de la connexion suivante.

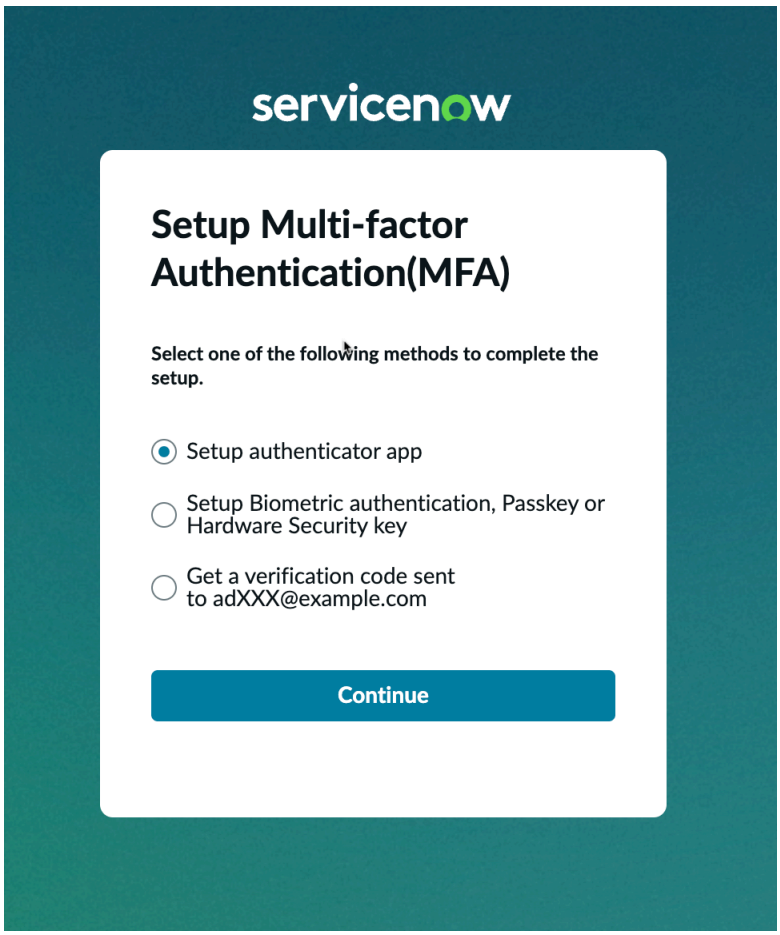
Procédure

1. Accédez à l’URL de votre instance pour ouvrir l’écran de connexion.
2. Entrez votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Se connecter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’écran d’authentification multifacteur s’affiche.



4. Sélectionnez l’une des méthodes pour terminer la configuration de la MFA.
   Pour plus d’informations sur chaque configuration, reportez-vous à la section Configurer l’authentification multifacteur pour la première fois.

   Si vous souhaitez reporter la configuration, sélectionnez **Reporter la configuration**. La durée maximale pendant laquelle vous pouvez différer la configuration s’affiche à l’écran et cette valeur est configurée par votre administrateur.

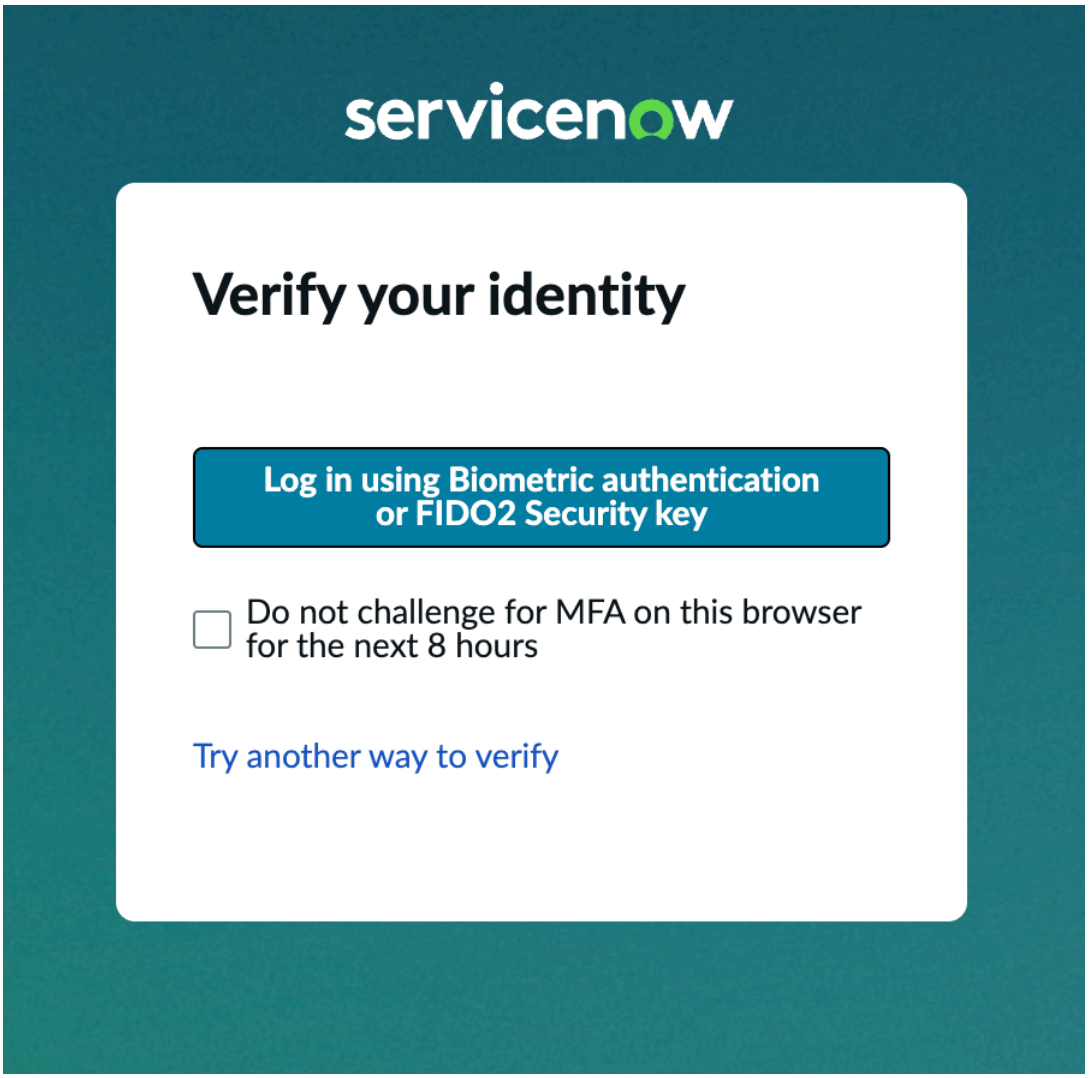
Résultats
Si vous avez déjà configuré l’authentification multifacteur, le facteur récemment utilisé s’affiche lorsque vous vous connectez à votre instance après avoir saisi votre nom d’utilisateur et votre mot de passe.

Example: Facteur MFA récemment utilisé

Si le facteur utilisé récemment était une connexion biométrique, lors de la connexion à l’aide de votre nom d’utilisateur et de votre mot de passe, vous êtes directement affiché sur l’écran de configuration de la MFA biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Applications d'authentification

Utilisez des applications d'authentification tierces pour générer des codes d'accès MFA temporaires.

Une application d'authentification est un logiciel tiers qui génère des codes d'accès temporaires. Vous pouvez utiliser ces codes secrets avec votre mot de passe pour vous connecter à une instance qui nécessite l'authentification multifacteur (MFA).

Si votre administrateur a activé la MFA sur votre instance, vous êtes invité à entrer un code secret après avoir saisi votre utilisateur et votre mot de passe lors de la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



ServiceNow nécessite des applications d'authentification qui prennent en charge les mots de passe uniques basés sur le temps (TOTP).

ServiceNow teste la MFA avec les authentificateurs suivants :

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

Remarque :
d'autres applications d'authentification non répertoriées peuvent également être compatibles, mais ne sont pas testées par ServiceNow.

Modifier une application d'authentification

Générez un nouveau code pour changer une application d'authentification sur votre appareil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vous devez avoir activé l’authentification multifacteur pour votre profil. Vous pouvez l’activer vous-même sur votre profil d’utilisateur ou votre administrateur peut l’activer pour vous.

Rôle requis : aucun

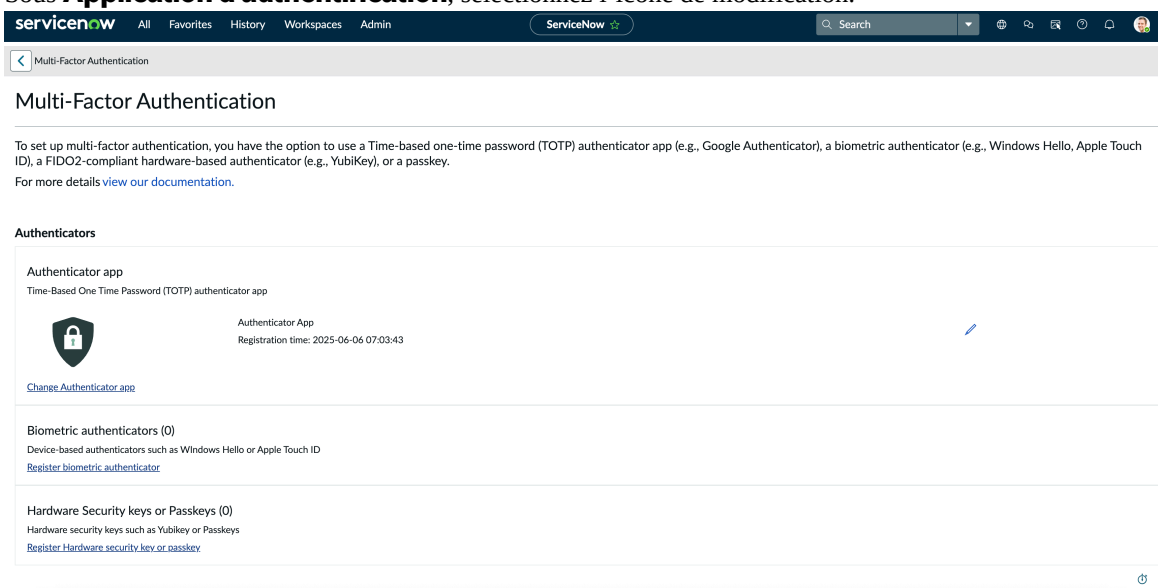
Procédure

1. Accédez à la **Tous** > **Libre-service** > **Mon profil**.

   Remarque :
   Vous pouvez également accéder à votre profil en cliquant sur votre nom d’utilisateur dans l’en-tête de l’instance.

2. Dans votre profil d’utilisateur, cliquez sur **Authentification multifacteur** dans la section **Liens connexes** .

3. Sous **Application d’authentification**, sélectionnez l’icône de modification.



4. Dans la fenêtre Modifier le code d’authentificateur, cliquez sur **Modifier**.

5. Suivez les instructions à l’écran pour enregistrer l’application d’authentification avec l’appareil.

Authentification Web

Vos utilisateurs peuvent utiliser des clés matérielles ou les lecteurs biométriques de leur appareil (FIDO2) pour s’authentifier à une instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clés matérielles



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.

Biométrie

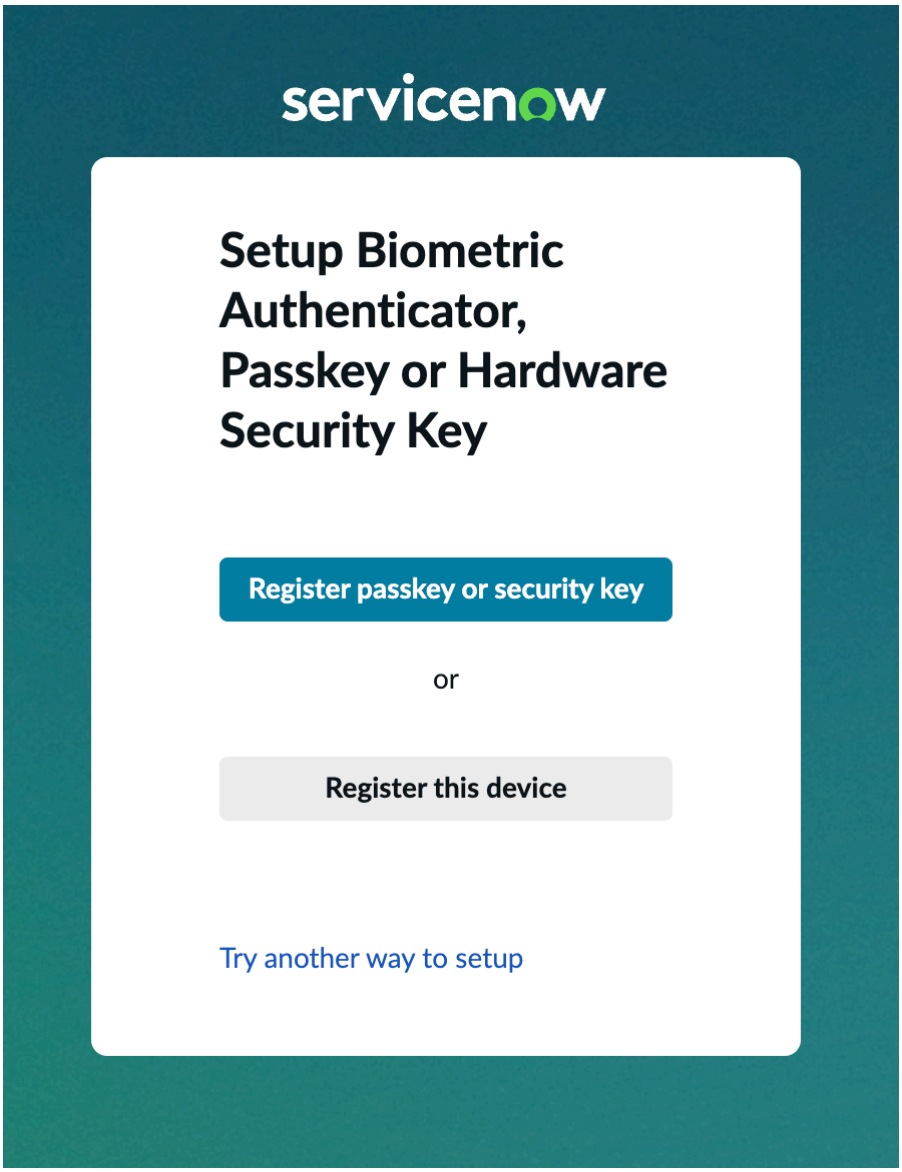


Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Choisissez le deuxième facteur que vous souhaitez authentifier et authentifiez-vous auprès de votre instance.



Pour configurer le module d'extension Authentification Web, reportez-vous à la section .

Enregistrer un authentificateur biométrique

Enregistrez un authentificateur biométrique à utiliser dans le cadre de votre connexion MFA.

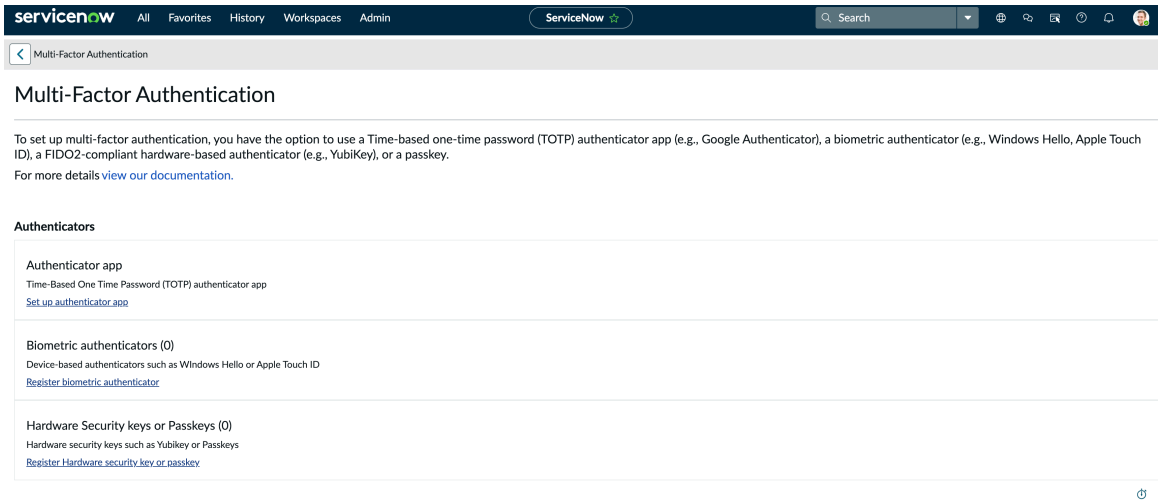
Avant de commencer
Rôle requis : aucun

Procédure

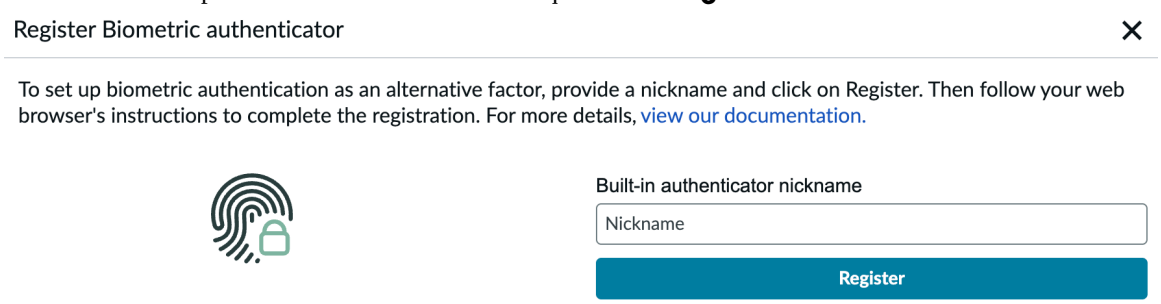
1. Accédez à la **Tous** > **Libre-service** > **Mon profil**.
2. Sous **Liens connexes**, cliquez sur **Authentification multifacteur**.
   La page d'authentification multifacteur s'ouvre.
3. Cliquez sur **Enregistrer l'authentification biométrique**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

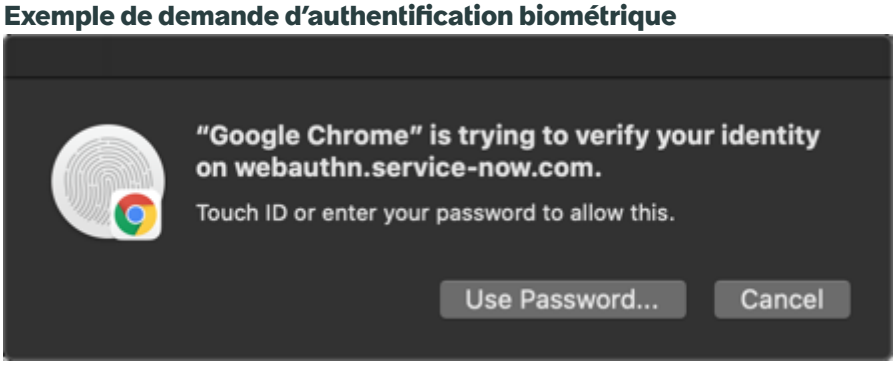


4. Entrez un surnom pour votre authentificateur et cliquez sur **Enregistrer**.



5. Lorsque vous y êtes invité, suivez les instructions à l'écran pour vous authentifier avec votre authentificateur biométrique.
Ce message varie en fonction de votre authentificateur spécifique.

Exemple de demande d'authentification biométrique



Une fois l'authentification réussie, une fenêtre de confirmation s'affiche. Cliquez sur X pour fermer la confirmation.

Résultats

Votre authentificateur biométrique est enregistré. Vous pouvez voir l'authentificateur biométrique répertorié sur la page Authentification multifacteur.

Enregistrer une clé de sécurité matérielle

Enregistrez une clé matérielle à utiliser dans le cadre de votre connexion MFA.

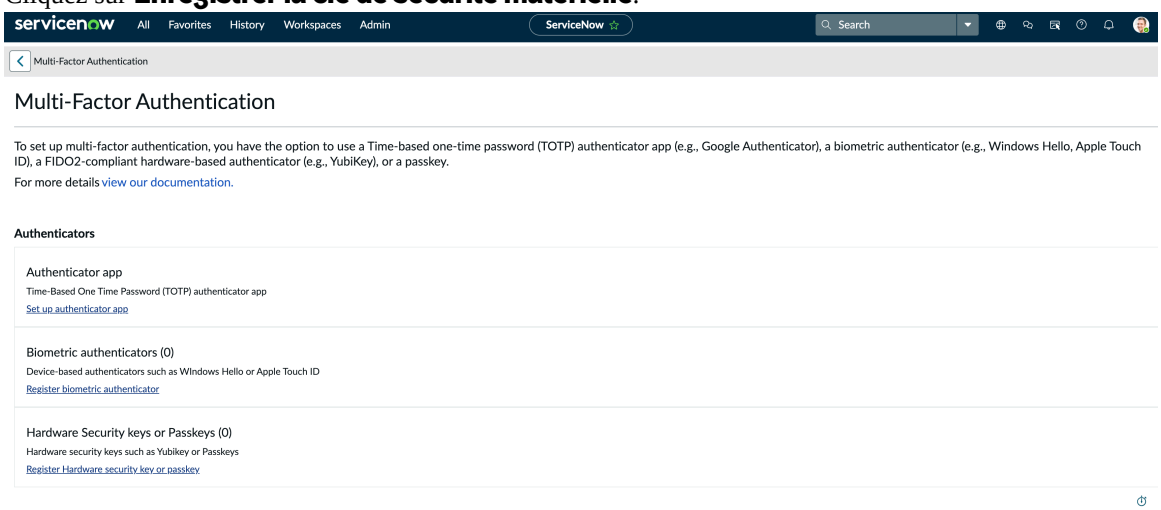
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

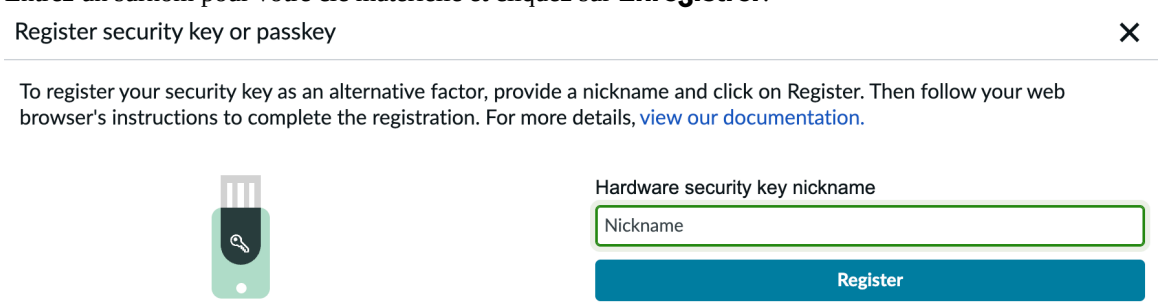
Avant de commencer
Rôle requis : aucun

Procédure

1. Accédez à la **Tous** > **Libre-service** > **Mon profil**.
2. Sous **Liens connexes**, cliquez sur **Authentification multifacteur**.
   La page Authentification multifacteur s'ouvre.
3. Cliquez sur **Enregistrer la clé de sécurité matérielle**.



4. Entrez un surnom pour votre clé matérielle et cliquez sur **Enregistrer**.



5. Lorsque vous y êtes invité, insérez votre clé de sécurité matérielle et activez-la.
   Une fois l'authentification réussie, une fenêtre de confirmation s'affiche. Cliquez sur X pour fermer la confirmation.

Résultats
Votre clé matérielle est enregistrée. La clé matérielle répertoriée dans la page Authentification multifacteur s'affiche.

Tableau de bord de MFA

Affichez les différentes mesures MFA pour comprendre l'adoption et l'utilisation de la MFA.

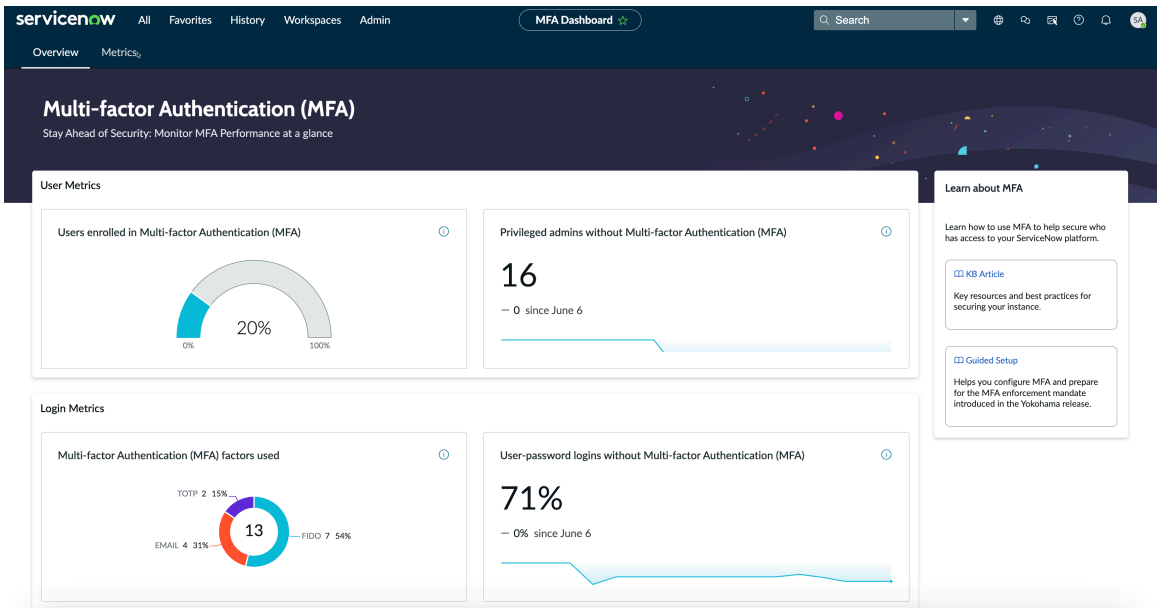
La MFA renforce la sécurité en exigeant une étape de vérification supplémentaire pendant le processus de connexion. Le tableau de bord MFA vous aide à surveiller et à gérer les paramètres MFA de votre organisation. Ce tableau de bord fournit une vue d'ensemble de l'inscription des utilisateurs de la MFA, des administrateurs privilégiés qui n'ont pas

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

opté pour la MFA et de la conformité. Vous pouvez l'utiliser pour vous assurer que tous les utilisateurs ont activé la MFA pour une sécurité renforcée.

Pour accéder au tableau de bord MFA, naviguez **Tous** > **Authentification multifacteur** > **Tableau de bord de MFA**.



Remarque :
Vous devez activer la MFA pour afficher les mesures. Pour plus d'informations, consultez Propriétés système de l'authentification multifacteur.

Voici les types de mesures affichées sur le tableau de bord MFA :

- Mesures utilisateur
- Mesures de connexion

Mesures utilisateur

La table suivante fournit des détails sur les mesures utilisateur dans le tableau de bord MFA.

Mesures utilisateur

Mesures	Description
Utilisateurs inscrits à l'authentification multifacteur (MFA)	Pourcentage d'utilisateurs pouvant effectuer une connexion basée sur nom d'utilisateur et mot de passe et inscrits à la MFA. Cette mesure fournit un aperçu de l'adoption de la MFA par les utilisateurs sur une période donnée. **Remarque :** Idéalement, le score devrait augmenter progressivement et devrait être de 100 % sur une période de temps (actualisé une fois par jour pour collecter les enregistrements d'un jour avant).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures utilisateur (suite)

Mesures	Description
Administrateurs privilégiés sans authentification multifacteur (MFA)	Les administrateurs privilégiés qui n'utilisent pas la MFA constituent un risque important pour la sécurité de la plateforme. Il est recommandé à ces personnes d'utiliser l'authentification multifacteur. **Remarque :** Les administrateurs privilégiés sont les utilisateurs qui ont au moins un rôle dans la table sys_icenter_role_config. (Actualisé une fois par jour pour collecter les enregistrements de la veille).

Mesures de connexion

La table suivante fournit des détails des mesures de connexion dans le tableau de bord MFA.

Mesures de connexion

Facteurs d'authentification multifacteur (MFA) utilisés	Classification des facteurs MFA utilisés lors de la connexion basée sur nom d'utilisateur et mot de passe.
Connexions par mot de passe de l'utilisateur sans authentification multifacteur (MFA)	Pourcentage de connexions basées sur nom d'utilisateur et mot de passe sans MFA. Cette mesure fournit un aperçu de l'adoption de la MFA sur une période donnée. **Remarque :** Idéalement, le score devrait diminuer progressivement et devrait être nul sur une période de temps (actualisé une fois par jour pour collecter les enregistrements de la veille).

Mesures utilisateur

Mesures utilisateur affiche les tendances d'inscription à la MFA de l'utilisateur sur ServiceNow.

Les mesures utilisateur sur le tableau de bord MFA sont les suivantes :

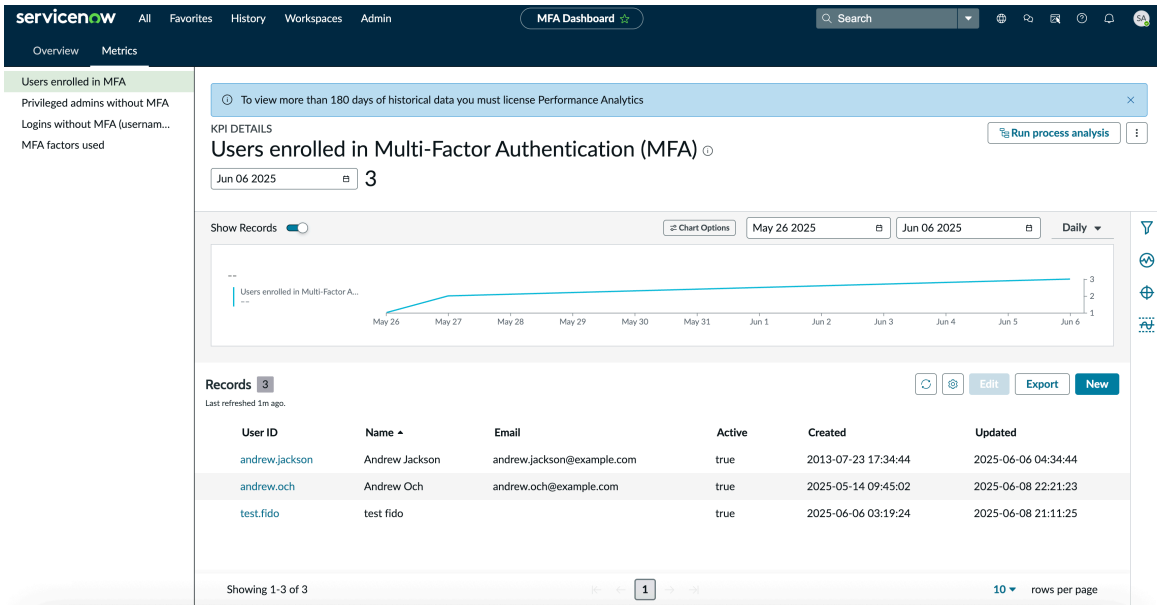
- Utilisateurs inscrits à l'authentification multifacteur (MFA)
- Administrateurs privilégiés sans authentification multifacteur (MFA)

Utilisateurs inscrits à l'authentification multifacteur (MFA)

Pourcentage d'utilisateurs pouvant effectuer une connexion basée sur nom d'utilisateur et mot de passe et inscrits à la MFA. Cette mesure fournit un aperçu de l'adoption de la MFA par les utilisateurs sur une période donnée.

Traduction automatique

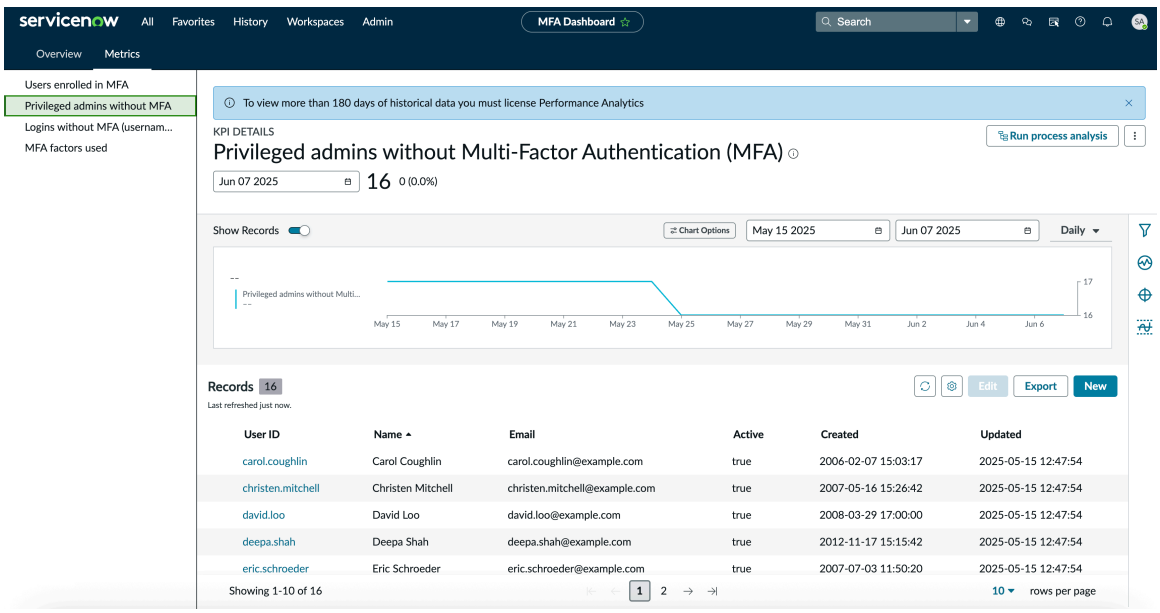
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Idéalement, le score devrait augmenter progressivement et devrait être de 100 % sur une période de temps (actualisé une fois par jour pour collecter les enregistrements d'un jour avant).

Administrateurs privilégiés sans authentification multifacteur (MFA)

Les administrateurs privilégiés qui n'utilisent pas la MFA constituent un risque important pour la sécurité de la plateforme. Il est recommandé à ces personnes d'utiliser l'authentification multifacteur.



Remarque :
Les administrateurs privilégiés sont les utilisateurs qui ont au moins un rôle dans la table **sys_icenter_role_config** . (Actualisé une fois par jour pour collecter les enregistrements de la veille).

Mesures de connexion

Mesures de connexion affiche les tendances de connexion sur le ServiceNow.

Les mesures de connexion sur le tableau de bord MFA sont les suivantes :

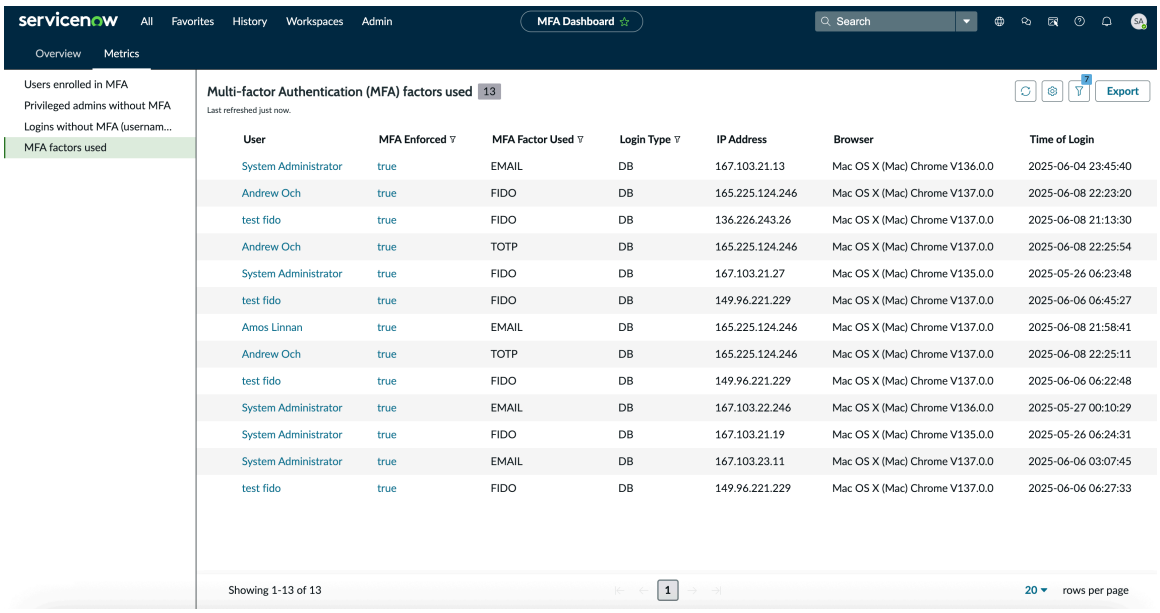
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Facteurs d'authentification multifacteur (MFA) utilisés
- Connexions par mot de passe de l’utilisateur sans authentification multifacteur (MFA)

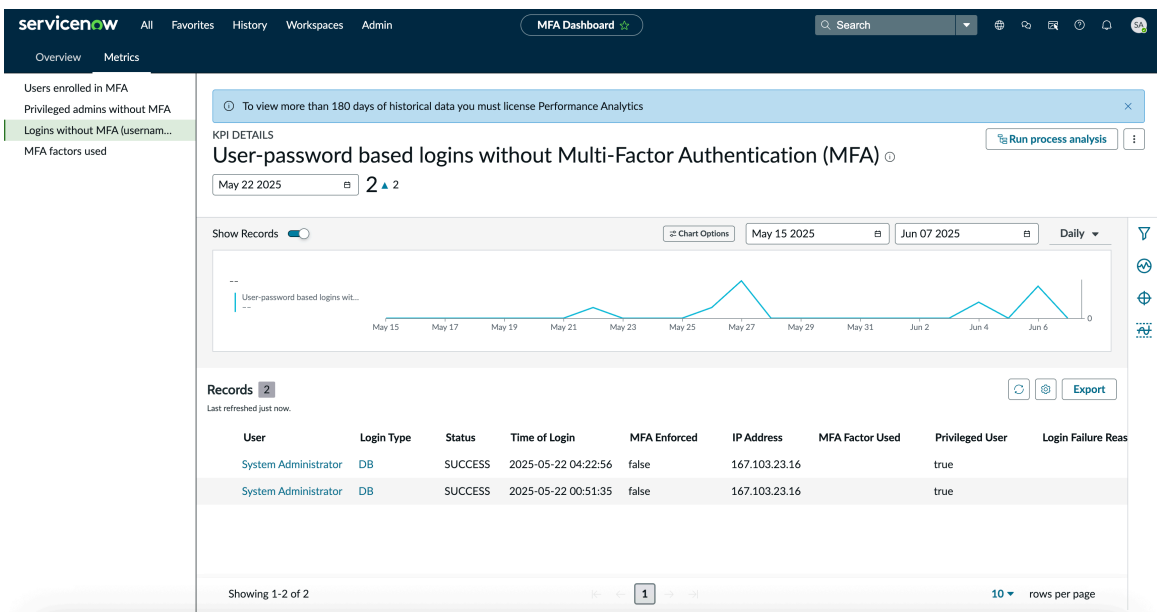
Facteurs d'authentification multifacteur (MFA) utilisés

Classification des facteurs MFA utilisés lors de la connexion basée sur nom d’utilisateur et mot de passe.



Connexions par mot de passe de l’utilisateur sans authentification multifacteur (MFA)

Pourcentage de connexions basées sur nom d’utilisateur et mot de passe sans authentification multifacteur. Cette mesure fournit un aperçu de l’adoption de la MFA sur une période donnée.



Remarque :
Idéalement, le score devrait diminuer progressivement et devrait être nul sur une période de temps (actualisé une fois par jour pour collecter les enregistrements de la veille).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

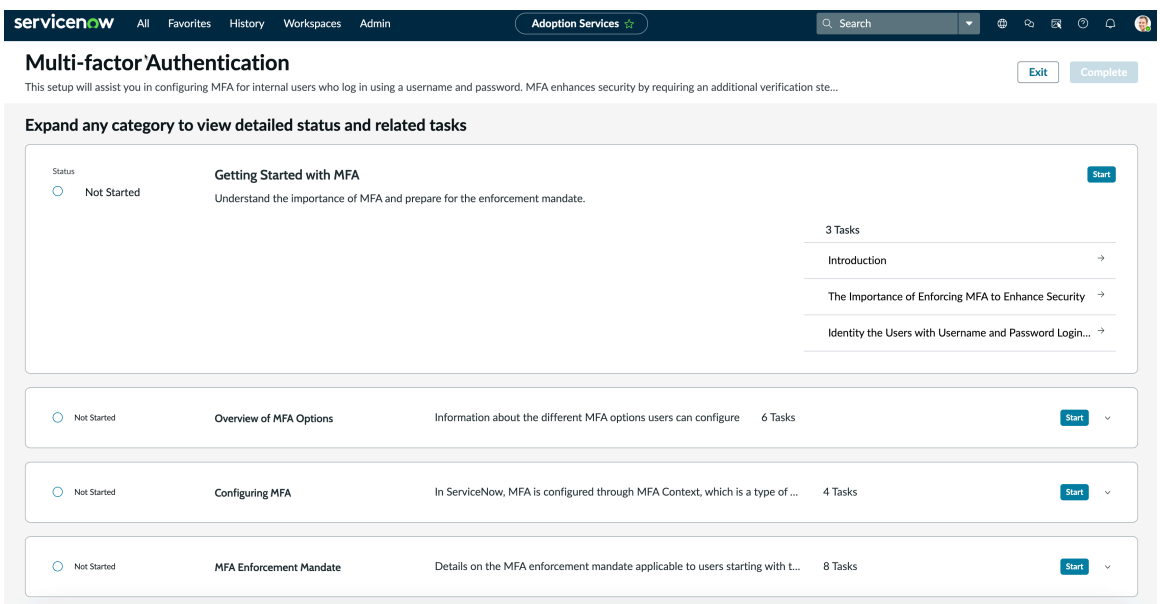
Configuration guidée de la MFA

Utilisez la configuration guidée de la MFA pour passer par la configuration initiale du module MFA et comprendre les exigences en matière d'application de la MFA.

La configuration guidée MFA vous aide à configurer l'authentification multifacteur pour les utilisateurs internes qui se connectent à l'aide d'un nom d'utilisateur et d'un mot de passe.

Pour accéder à la configuration guidée MFA, accédez à **Tous** > **Services d'adoption** > **Configuration guidée**. Vous pouvez choisir **Toutes les applications** , puis **Authentification multifacteur**.

La configuration guidée de l'authentification multifacteur s'ouvre dans un nouvel onglet. Développez n'importe quelle catégorie pour afficher l'état détaillé et les tâches connexes sur la page affichée.



Effectuez la tâche suivante pour vous familiariser avec les configurations MFA :

- Mise en route de la MFA
- Vue d'ensemble des options MFA
- Configuration de la MFA
- Mandat d'application de la MFA
- Communication utilisateur et intégration
- Surveillance

Pour en savoir plus sur l'utilisation de la configuration guidée, reportez-vous à la section Guided Setup .

Authentification unique (SSO) de plusieurs fournisseurs

L'authentification unique externe permet aux organisations d'utiliser plusieurs fournisseurs d'identité SSO (IdP) pour gérer l'authentification et conserver l'authentification de base de données locale (de base).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’authentification unique (SSO) de plusieurs fournisseurs est une méthode d’authentification qui permet aux utilisateurs d’accéder à plusieurs applications avec un seul identifiant et un seul ensemble d’informations d’identification.

Pour utiliser SSO, vous devez comprendre ce qui suit :

- *`Service Providers`*: lorsque les utilisateurs qui tentent d’accéder à l’instance ServiceNow sont redirigés vers un fournisseur d’identité (IdP) pour valider leurs informations d’identification après une validation réussie, les utilisateurs sont autorisés à accéder à l’instance. Ici, ServiceNow agit en tant que fournisseur de service et s’appuie sur un fournisseur d’identité (IdP) pour gérer l’authentification utilisateur et accorder l’accès à l’instance.
- Fournisseurs d’identité : les IdP sont des systèmes externes qui valident l’identité et les informations d’identification des utilisateurs pour accéder à un système.

Pour établir une SSO avec pour accéder ServiceNowà , vous devez activer le SSO (Multi-provider Single sing-on), vous devez installer le module d’extension *`Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer)`* . Pour plus d'informations, consultez Activer le module d’extension SSO de plusieurs fournisseurs.

Une fois l’installation du module d’extension réussie, vous pouvez personnaliser les propriétés SSO, les tables d’accès et les scripts fournis avec le module d’extension. Pour plus d'informations, consultez Propriétés, tables et scripts SSO de plusieurs fournisseurs.

ServiceNow prend en charge les méthodes SSO suivantes :

- OpenID Connect
- SAML 2.0
- Authentification Digest (authentification basée sur les jetons).

Choisissez la méthode SSO en fonction de vos besoins et apprenez-en plus sur la façon dont vous devez vous préparer à la configuration de SSO. Vous devez effectuer plusieurs étapes pour configurer l’authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création des fournisseurs d’identité (IdP) et la configuration des utilisateurs pour utiliser SSO. Pour plus d'informations, consultez Configurations SSO de plusieurs fournisseurs.

Une fois la configuration réussie, les IdP actifs dans l’instance sont répertoriés sur le .ServiceNow Vous pouvez répertorier différents fournisseurs d’identité (IdP) SAML ou OIDC.

Remarque :
Un maximum de 10 IdP peut être répertorié sur la page de connexion. Les options IdP ne sont pas visibles si le module d’extension Prise en charge de domaine - Domain Extensions Installer (*`com.glide.domain.msp_extensions.installer`*) est installé et activé sur l’instance.

La version Zurich de ServiceNow inclut les améliorations suivantes sur l’authentification unique :

- **Répertorier les IdP SAML sur la page de connexion** : connectez-vous à l’aide des IdP SAML et OIDC répertoriés dans l’expérience de connexion sur les pages de connexion de la plateforme et du portail, ce qui permet aux utilisateurs de sélectionner plus facilement leur IdP préféré. Auparavant, seuls les IdP de l’OIDC étaient répertoriés.
- **Sélectionner un groupe pour la mise en service automatique** : sélectionnez des groupes spécifiques pendant la configuration de mise en service automatique pour SAML et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

OIDC, en veillant à ce que les utilisateurs soient automatiquement affectés aux groupes appropriés.

- **Configurer plusieurs enregistrements OIDC à l'aide de la même URL connue** : simplifiez la configuration d'OIDC en permettant la création d'enregistrements OIDC à l'aide de la même URL connue, rationalisant ainsi le processus de configuration.
- **Amélioré Page complète de déconnexion externe** : affichage du motif d'échec de la connexion à l'utilisateur. Mise en service pour se reconnecter ServiceNow sur la page de déconnexion externe terminée en cas de déconnexion réussie.
- **Message d'erreur amélioré** : affichage du message d'erreur générique en cas d'échec de la déconnexion unique (SLO), assurant une communication cohérente et sécurisée.
- **Améliorations de la notification pour le magasin de clés de chiffrement et de certificat SAML** : recevez des notifications en temps opportun aux administrateurs pour l'expiration des mises à jour du magasin de clés de chiffrement et de certificat SAML, en veillant à ce que vos configurations SSO restent sécurisées et à jour.

Example: Pourquoi l'organisation a-t-elle besoin de l'authentification unique ?

Une entreprise dispersée dans le monde entier peut exiger un fournisseur SSO pour ses employés, un autre pour ses fournisseurs et une authentification de base de données locale pour ses administrateurs. Une entreprise peut également implémenter SAML 2.0 et des solutions d'authentification par jeton de synthèse sur la même instance.

Activer le module d'extension SSO de plusieurs fournisseurs

Cette intégration nécessite le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).

Avant de commencer

Rôle requis : admin.

Le module d'extension com.snc.integration.sso.multi.installer peut également être utilisé pour OIDC, SAML et Digest.

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Propriétés, tables et scripts SSO de plusieurs fournisseurs

Le module d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs inclut les propriétés système, les tables et les scripts suivants.

Propriétés

L'authentification unique de plusieurs fournisseurs ajoute les propriétés système suivantes.

Propriétés SSO de plusieurs fournisseurs

Nom	Description
glide.authenticate.multisso.debug	Active (vrai) ou désactive (faux) la journalisation de débogage pour l'intégration SSO de plusieurs fournisseurs. • Type : true | false • Valeur par défaut : faux
glide.authenticate.multisso.enabled	Active (vrai) ou désactive (faux) l'authentification unique (SSO) de plusieurs fournisseurs. • Type : true | false • Valeur par défaut : faux **Remarque :** Définir cette propriété sur faux ne désactive pas l'authentification unique (SSO) de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, l'ACR doit également être désactivé à l'aide de la *glide.sso.acr.enabled* propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.
glide.authenticate.multissov2_feature.enabled	Cette propriété détermine si la version MultiSSOv2 est activée dans l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés SSO de plusieurs fournisseurs (suite)

Nom	Description
`glide.authenticate.show.max.sso.login.option`	Cette propriété détermine le nombre maximal d'options SSO affichées sur l'écran de connexion. **Remarque :** La valeur par défaut est 5. La valeur maximale de la propriété est de 10.
`glide.authenticate.show.max.sso.login.option`	Cette propriété détermine le nombre maximal d'IdP affichés sur l'écran de connexion. « glide.authenticate.show.max.sso.login.option » **Remarque :** La valeur par défaut est de 10.

Tables

L'authentification unique de plusieurs fournisseurs ajoute les tables suivantes.

Tables SSO de plusieurs fournisseurs

Nom	Description
Propriétés SSO [sso_properties]	Stocke les données de chaque fournisseur d'identités, schémas, données SSO communes, et ainsi de suite.
Propriétés SAML 2 Update 1 [saml2_update1_properties]	Stocke les données des configurations SAML 2.0 Update 1 telles que les certificats SAML.
Propriétés Digest [digest_properties]	Stocke les données pour les configurations d'authentification par jeton de synthèse.
Fédération SSO [sso_federation]	Stocke les données de chaque fédération SSO.
Fournisseur d'identité OIDC [oidc_identity_provider]	Stocke les données des fournisseurs d'identité basés sur Open ID Connect.

Scripts

L'authentification unique (SSO) de plusieurs fournisseurs ajoute les scripts suivants.

Scripts SSO de plusieurs fournisseurs

Nom	Description
SSO à fournisseurs multiples	Permet à un client d'avoir un type SSO défini sur la base d'une société.
MultiSSOLogin	Permet à chaque domaine d'avoir son propre script de connexion.
MultiSSOLogout	Permet à chaque domaine d'avoir son propre script de déconnexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scripts SSO de plusieurs fournisseurs (suite)

Nom	Description
MultiSSO_OIDC_custom	Permet à un utilisateur de définir un script d'authentification unique personnalisé pour la connexion OIDC.
MultiSSO_OIDC_logout_custom	Permet à un utilisateur de définir un script de déconnexion personnalisé pour la connexion OIDC.
MultiSSO_Abstract_Core	Fournit une classe de base pour toutes les classes SSO de plusieurs fournisseurs.
MultiSSO_ClientHelper	Fournit des fonctions d'utilitaire appelables par le client pour l'authentification unique (SSO) de plusieurs fournisseurs.
MultiSSO_DigestedToken	Fournit une logique de système de base pour l'authentification par jeton digéré.
MultiSSO_SAML2_Update1	Fournit une logique pour traiter l'authentification SAML 2.0 Update 1 pour une authentification unique mutualisée.

Configurations SSO de plusieurs fournisseurs

Vous devez effectuer plusieurs étapes pour configurer l'authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création des fournisseurs d'identité (IdP) et la configuration des utilisateurs pour utiliser SSO.

Consultez les rubriques suivantes pour en savoir plus sur chacune des configurations.

- Flux d'authentification IdP SSO de plusieurs fournisseurs (SAML)
- Configurer les propriétés SSO de plusieurs fournisseurs
- Créer un fournisseur d'identité externe
- Configurer les utilisateurs pour l'authentification unique (SSO) de plusieurs fournisseurs

Configurer les propriétés SSO de plusieurs fournisseurs

Configurez les propriétés SSO et ajoutez une propriété à la table Propriétés système pour configurer une liste d'inclusion IdP.

Avant de commencer
Rôle requis : admin

Procédure

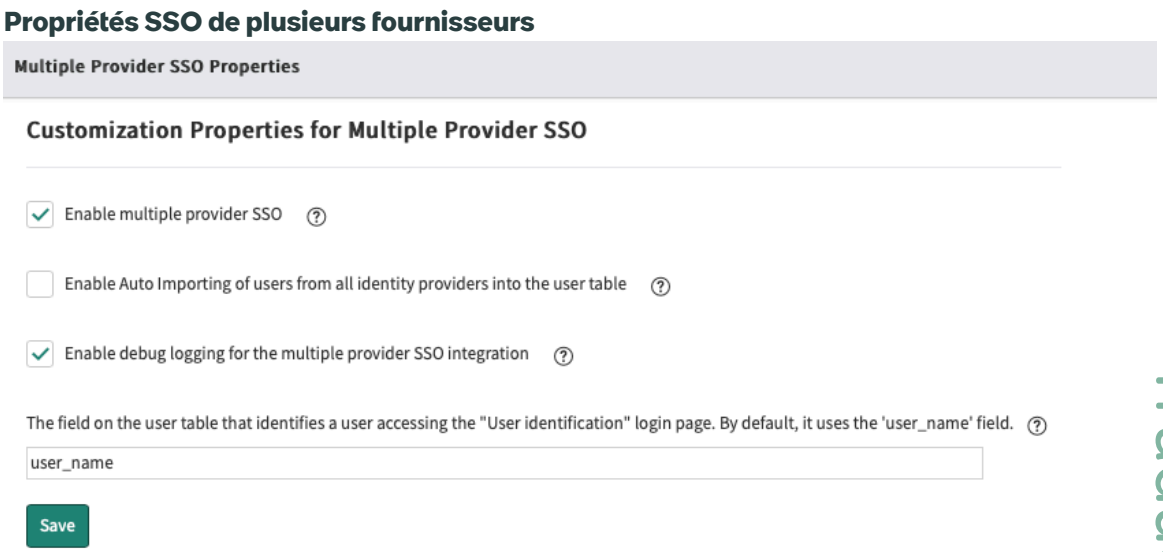
1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Administration** > **Propriétés**.
2. Cochez la case **Activer l'authentification unique (SSO) de plusieurs fournisseurs** .
   Cette sélection ajoute le lien Utiliser une connexion externe à la page de connexion.
3. Pour mettre à jour la table utilisateur avec les utilisateurs dans IdP, sélectionnez l'option **Activer l'importation automatique** .
4. Pour permettre aux messages de débogage d'apparaître au bas du cadre de contenu, cochez la case **Activer la journalisation du débogage pour l'intégration SSO de plusieurs fournisseurs** .
   Si elle est activée, la fonctionnalité de journalisation de débogage ralentit les performances et utilise l'espace disque pour générer des journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la propriété **Champ de la table utilisateur qui identifie un utilisateur accédant à la page de connexion d'identification de l'utilisateur**, saisissez le champ de la table Utilisateur qui contient la valeur que l'IdP utilise pour identifier l'utilisateur. La valeur par défaut est **user_name**.

   La valeur par défaut est **user_name**.



6. Cliquez sur **Enregistrer**.
7. Demandez à vos utilisateurs de cliquer sur le lien **Utiliser une connexion externe** lorsqu'ils se connectent à l'instance.

Information associée

Attribution d'utilisateurs SAML

Créer un fournisseur d'identité externe

Une fois que vous avez configuré les propriétés SSO de plusieurs fournisseurs, vous pouvez mettre à jour ou créer un nouveau fournisseur d'identité SAML 2.0 ou de jeton de synthèse.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Pour modifier un enregistrement de fournisseur d'identité, cliquez sur l'enregistrement.
   - Pour les configurations de jeton de synthèse, mettez à jour manuellement les propriétés.
   - Pour les configurations SAML2 Update 1, mettez à jour automatiquement les métadonnées du fournisseur d'identité avec le lien connexe **Importer les métadonnées du fournisseur d'identité** ou mettez à jour les propriétés manuellement.
   - Pour les configurations OpenID Connect, mettez à jour manuellement les propriétés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Pour créer un nouveau fournisseur d'identité, cliquez sur **Nouveau**.
   - Pour les configurations de jeton de synthèse : cliquez sur **SSO de synthèse** et saisissez les propriétés de synthèse pour l'authentification unique de plusieurs fournisseurs.
   - Pour les configurations SAML2 : cliquez sur **MultiSSOV2_SAML2_custom** et importez les métadonnées du fournisseur d'identité à partir d'une URL, au format XML, ou saisissez manuellement les informations du fournisseur d'identité.



   - Pour OpenID Connect : cliquez sur **OpenID Connect** et saisissez l'ID client, le secret client et l'URL de configuration connue.

4. Pour faire de l'IdP l'IdP de basculement utilisé lorsque l'IdP par défaut n'est pas disponible, cochez la case **Par défaut** .

   Si SAML 2 Update 1 est actif et que vous effectuez une mise à niveau vers la version Fuji, l'IdP SAML 2 Update 1 est sélectionné comme basculement par défaut. Aucun IdP de basculement par défaut n'est sélectionné pour les nouvelles instances ou si vous effectuez une mise à niveau à partir d'une version sur laquelle SAML 2 Update 1 n'est pas active.

   Remarque :
   Le processus d'importation des métadonnées crée automatiquement un enregistrement de certificat pour le fournisseur d'identité. Accédez au module **Certificat x509** pour voir le certificat.

   Remarque :
   Les certificats pour l'authentification unique doivent toujours être au format PEM pour fonctionner avec les certificats SAML.

5. Si Signature électronique est actif, configurez le formulaire Fournisseur d'identité et ajoutez le champ **URL de consommateur d'assertion pour l'authentification de signature électronique** .
   Dans la plupart des cas, cette URL est : https://YOURINSTANCE.service-now.com/consumer.do. Toutefois, si vous utilisez une méthode personnalisée de gestion de l'authentification SAML pour les signatures électroniques, vous pouvez configurer votre propre URL de consommateur. Si vous utilisez uniquement SAML 2.0 Update 1 et non l'authentification unique multi-fournisseurs, configurez l'URL de consommateur d'assertion avec les propriétés SAML de signature électronique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Générer les métadonnées du fournisseur de service d'instance (SP) pour SAML

Dans le cadre de votre configuration SSO, vous pouvez générer les métadonnées SP d'instance à fournir à l'IdP.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'IdP a besoin des métadonnées du SP d'instance pour s'authentifier et transmettre les demandes.

Procédure

1. Choisissez votre module d'extension SSO installé :

Option	Description
Authentification unique (SSO) de plusieurs fournisseurs	Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**. Choisissez un IdP et cliquez sur le bouton **Générer les métadonnées** . L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres de propriété système.
SAML 2 SSO	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres de propriété système.

2. Copiez les métadonnées SP dans la zone de texte.

   Par exemple :

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Fournissez les métadonnées du SP d'instance à l'IdP.
   Par exemple, SSOCircle permet à un utilisateur de fournir les métadonnées SP en ligne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les utilisateurs pour l'authentification unique (SSO) de plusieurs fournisseurs

Les administrateurs peuvent configurer l'authentification unique (SSO) de plusieurs fournisseurs pour des utilisateurs individuels ou pour tous les utilisateurs qui appartiennent à une société. Vous ne pouvez pas configurer l'authentification unique (SSO) de plusieurs fournisseurs pour les groupes.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Cliquez avec le bouton droit sur un enregistrement de fournisseur d'identité, puis sélectionnez **Copier sys_id**.
3. Copiez les données dans votre presse-papiers.
4. Accédez à un enregistrement d'utilisateur ou à un enregistrement de société.
5. Configurez le formulaire et ajoutez le champ **Source SSO** .
6. Dans le champ **Source SSO** , entrez l'une des options suivantes :
   - **Utilisateurs SAML** : entrer **SSO :** suivi de la sys_id de l'enregistrement du fournisseur d'identité.
   - **SSO Utilisateurs de fédération** : entrez **la fédération :** suivie de l'sys_id de l'enregistrement de la fédération.
7. Cliquez sur **Mettre à jour**.

Tester les connexions IdP

Le test de la connexion à un fournisseur d'identités valide les paramètres avant d'activer l'authentification externe.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La version Jakarta prend en charge la connexion de test dans une fenêtre contextuelle. Si votre IdP ne fonctionne pas correctement avec cette option, vous pouvez désactiver ce paramètre par défaut.
La tâche Actualiser les métadonnées IdP MultiSSO extrait et met à jour le certificat pour l'IdP lors de la création, de la mise à jour ou du test de la connexion.

Remarque :
Dans certains cas d'IdP, en cas d'échec de la connexion test, l'utilisateur doit créer glide.authenticate.multisso.test.connection.mandatory avec la valeur false et vous pouvez activer l'IdP sans le test de la connexion.

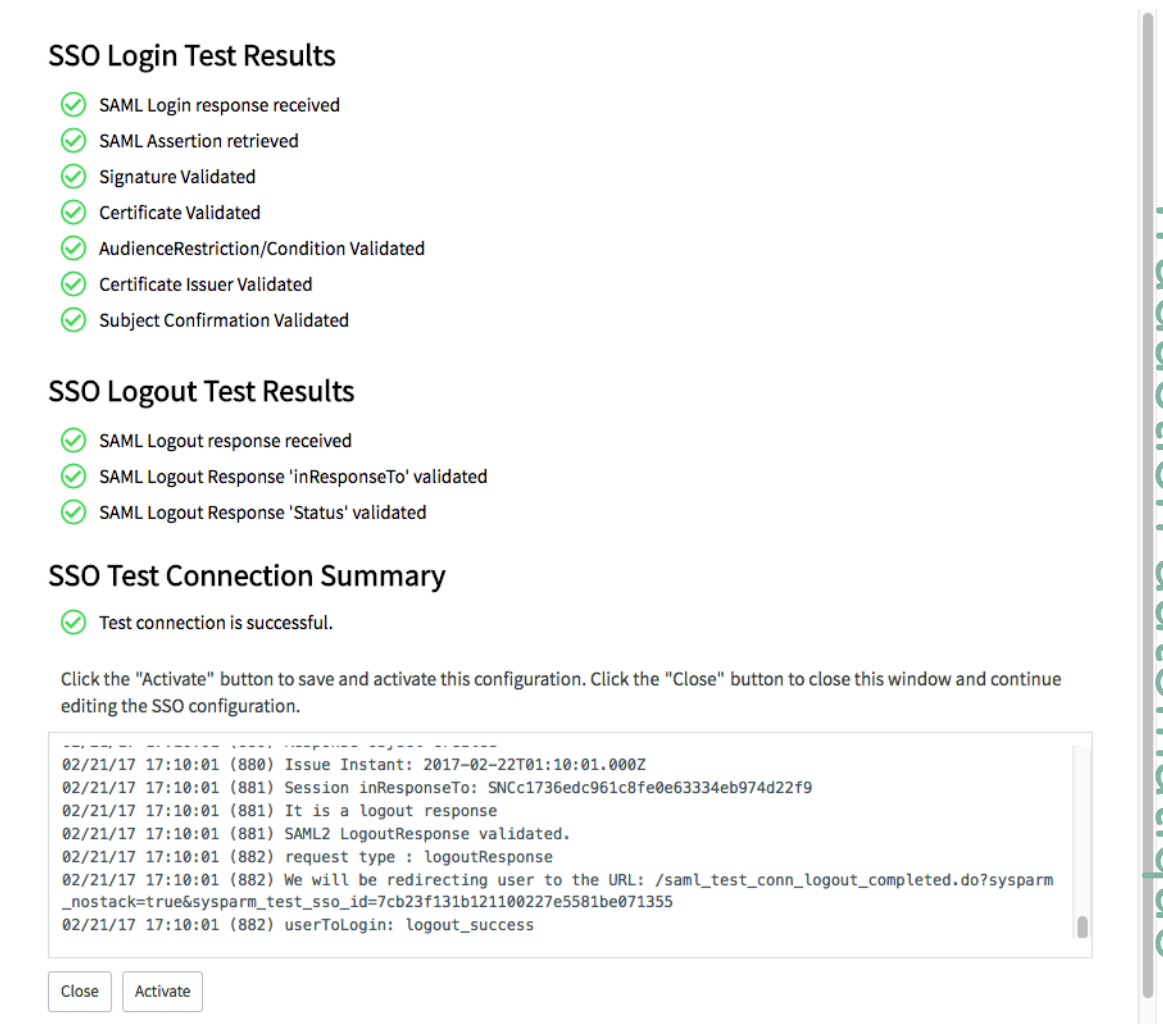
Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sélectionnez un IdP défini ou cliquez sur **Nouveau** pour en définir un nouveau.
3. **Facultatif :** Configurer un fournisseur d'identité en cas de configuration d'un nouvel IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Test de la connexion** et saisissez les informations d'identification de connexion pour que l'IdP vérifie la connexion.
   Vous ne pouvez pas activer l'IdP tant que vous n'avez pas réussi à tester la connexion. Si le test échoue, vous pouvez effectuer la mise à jour pour enregistrer vos informations de configuration, mais vous ne pouvez pas activer cette configuration.
5. Vérifiez les résultats à l'aide de la section **Résultats/Résumé des tests SSO** ou **Journaux SSO des tests** pour afficher les messages du journal.
   En cas d'erreurs, reportez-vous au Erreurs et correctifs Multi-SSO (SAML 2.0)
6. Cliquez sur **Annuler** lorsque le test est terminé.



Traduction automatique

Erreurs courantes de connexion IdP

Le tableau suivant décrit certaines des erreurs de connexion IdP courantes et leurs solutions.

Dépannage des connexions de test IdP

Messages d'erreur	Solution
Échec de la validation du champ d'utilisateur. Le champ d'utilisateur « <nom du champ > » n'est pas un champ de sys_user table.	Vérifiez que le contenu du champ de table d'utilisateur que vous avez sélectionné correspond au jeton NameID SAML.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage des connexions de test IdP (suite)

Messages d'erreur	Solution
L'émetteur de l'assertion n'est pas valide.	Vérifiez que **l'URL du fournisseur d'identité** contient une URL valide pour votre fournisseur d'identité. Chaque URL IdP doit être unique.
Échec de la validation de AudienceRestriction.	Vérifiez que **l'URI d'audience** contient une URL valide vers votre instance.
Impossible de se déconnecter de la session d'IdP.	Vérifiez que l'URL **SingleLogoutRequest** contient une URL valide vers le service de déconnexion de votre fournisseur d'identités.
La signature n'a pas été validée par rapport à la clé des informations d'identification.	Vérifiez que l'IdP dispose d'un certificat valide.

Résoudre les problèmes de script avec SAML

Résolvez les problèmes de script avec SAML. Vous pouvez rencontrer des problèmes de script si SAML est déjà actif au moment de l'activation de l'authentification unique multiple et si vous avez déjà personnalisé l'installation se termine.

Avant de commencer
Rôle requis : admin

Procédure

1. Sauvegardez le SAML2SingleSignon_update1 de sortie d'installation modifié et l'include de script SAML2_update1.
2. Rétablissez la sortie d'installation et l'include de script à la version disponible avec le système de base de référence.
3. Activez ou mettez à niveau le module **d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** .
   Le système met à niveau SAML et tous les fichiers nécessaires vers SAML 2 Update 1.
4. Ouvrez la page Propriétés SSO multiples et cochez la case **Activer l'authentification unique (SSO) de plusieurs fournisseurs** pour l'activer.
5. Placez les changements de sortie d'installation SAML2SingleSignon_update1 dans le MultiSSO_SAML2_Update1 d'inclusion de script de base **de référence et les changements d'include de script de SAML2_update1** dans l'include de script de SAML2_update1 de base de référence.

Se connecter à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs

La méthode recommandée et la plus efficace pour que les utilisateurs se connectent à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs consiste à utiliser une URL spécialement configurée.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Une fois l'authentification unique (SSO) de plusieurs fournisseurs configurée, vous pouvez envoyer une URL à vos utilisateurs avec l'IdP correct dans la chaîne de paramètre. Par exemple :

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois qu'un utilisateur s'est connecté à la page IdP, un cookie contenant le sys_id IdP est ajouté au navigateur. La prochaine fois que l'utilisateur tente de se connecter, le système le redirige vers le serveur IdP, qui se connecte automatiquement à l'instance.

Si un paramètre d'URL n'est pas défini ou si le cache du navigateur a été effacé, les utilisateurs peuvent également effectuer les opérations suivantes :

Procédure

1. Cliquez sur le lien **Utiliser une connexion externe** sur la page de connexion.

   La page de connexion externe s'affiche. Les utilisateurs peuvent cliquer sur **Utiliser la connexion locale** pour revenir à la page de connexion standard.

2. Saisissez la valeur du champ spécifié dans la table utilisateur que vous avez configuré dans les propriétés SSO de plusieurs fournisseurs.

   L'utilisateur est redirigé vers le serveur IdP, où il se connecte.

Résultats

Une fois que les utilisateurs se sont connectés à un fournisseur d'identités, ils sont automatiquement redirigés vers ce fournisseur d'identités chaque fois qu'ils tentent d'accéder à l'instance. Pour qu'un utilisateur accède à un autre IdP, envoyez à l'utilisateur une URL avec les nouvelles informations d'IdP dans le paramètre. Le nouvel IdP remplace l'ancien IdP dans le cookie si l'utilisateur se connecte avec succès. Si l'utilisateur ne se connecte pas avec succès, les anciennes informations IdP sont conservées dans le cookie.

Permettre aux utilisateurs de choisir le fournisseur d'identité pour la connexion

La prise en charge de la fédération SSO permet aux utilisateurs de choisir à quel IdP se connecter.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les fédérations SSO regroupent les métadonnées de plusieurs fournisseurs d'identités et fournisseurs de services, y compris votre instance. Les fédérations publient ensuite les métadonnées sous la forme d'un fichier XML, qui comprend des informations telles que les noms IdP et les certificats IdP. Les administrateurs peuvent ensuite demander à l'instance de lire le fichier XML et remplir automatiquement la table Propriétés SSO avec toutes les informations IdP nécessaires.

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fédération**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient (voir la table).
4. Cliquez sur **Envoyer**.
5. Après avoir configuré une fédération, activez la tâche planifiée Actualiser les métadonnées SSO, puis configurez les utilisateurs auxquels vous souhaitez donner accès aux IdP de fédération. Utilisez les sys_ID de l'enregistrement de fédération que vous venez de créer.

   Utilisez le sys_ID de l'enregistrement de fédération que vous venez de créer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'instance remplit la table des propriétés SSO avec les informations IdP. Lorsque les utilisateurs configurés pour utiliser la fédération se connectent, ils sont redirigés vers l'URL du service de découverte que vous avez configurée. Ensuite, ils sélectionnent l'IdP et fournissent les informations d'identification nécessaires. Vous pouvez également envoyer aux utilisateurs une URL avec l'IdP dans le paramètre.

Permettre aux utilisateurs de choisir le fournisseur d'identité pour la connexion

Champ	Description
Nom	Saisissez un nom descriptif pour la fédération.
Actif	Cochez la case pour permettre à l'instance d'extraire le fichier XML de la fédération.
Type	Sélectionnez le type d'authentification pris en charge par cette fédération.
Découverte Service URL	Entrez l'URL du service de découverte pour cette fédération. Il s'agit du site où les utilisateurs sont invités à sélectionner un IdP et à se connecter.
URL des métadonnées	Entrez l'URL du fichier XML qui contient les métadonnées de fédération.
Certificat x509	Sélectionnez le certificat de fédération.
Domaine	Sélectionnez le domaine auquel les données appartiendront.

Remarque :
L'IdP de gestion d'identité fédérée InCommon est préconfiguré.

À utiliser Portail de services avec l'authentification unique (SSO) de plusieurs fournisseurs pour rediriger une URL

Portail de services utilise une combinaison de propriétés système et d'includes de script pour déterminer comment le système gère les redirections d'URL pour les utilisateurs qui se connectent au portail.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Si vous utilisez la propriété système pour être automatiquement redirigé vers votre fournisseur d'identité (IdP) principal, vous Portail de services serez automatiquement redirigé vers ce fournisseur d'identité. Si vous avez plusieurs fournisseurs d'identité, Portail de services affiche un lien sur la page de connexion pour **utiliser une connexion externe**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Configurer la page de connexion du portail de services
2. Rediriger vers Portail de services après la connexion

Récupération de compte (ACR)

Les administrateurs peuvent configurer la récupération de compte (ACR) pour effectuer des activités de récupération telles que le traitement d'une erreur de configuration SSO ou de certificats expirés.

Remarque :
L'activation d'ACR désactive les connexions interactives locales (basées sur le nom d'utilisateur ou le mot de passe) lorsque la SSO est activée pour vos instances.

ACR fournit les options suivantes :

- Contournez votre connexion d'authentification unique (SSO) pour résoudre les problèmes liés à la configuration SSO en tant qu'administrateur.
- Connectez-vous à l'aide de l'authentification unique (SSO) pour effectuer des tâches avec un compte administrateur configuré comme une récupération de compte.
- Les flux ACR permettent aux administrateurs d'utiliser des options en libre-service pour traiter la récupération de compte lorsqu'il y a un besoin de récupération, par exemple, SSO : configuration incorrecte, certificats expirés.
- Réduisez les accès non autorisés à l'instance et fournissez une base solide pour utiliser ACR en dehors des cas d'utilisation SSO.

Nouvelle instance

Pour qu'une nouvelle instance utilise ACR, vous devez procéder comme suit :

- Activez le module d'extension Authentification unique (`com.snc.integration.sso.multi.installer`)
- Activer ACR (`glide.sso.acr.enabled`) : cette option est activée par défaut en cas d'instance nouvelle.
- Avant d'activer la propriété SSO (`glide.authenticate.multisso.enabled`), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.

  Remarque :
  Définir cette propriété sur faux ne désactive pas l'authentification unique (SSO) de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, l'ACR doit également être désactivé à l'aide de la `glide.sso.acr.enabled` propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.

- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer la MFA avant de s'inscrire en tant qu'utilisateur ACR.

Instance mise à niveau

Pour qu'une instance mise à niveau utilise ACR, vous devez procéder comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le module d'extension Authentification unique (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled)

Remarque :
En cas d'instance mise à niveau, l'administrateur doit activer ACR.

- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.
- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer la MFA avant de s'inscrire en tant qu'utilisateur ACR.

Configurer les utilisateurs de récupération de compte

Pour utiliser la récupération de compte, vous devez enregistrer au moins un compte administrateur en tant qu'utilisateur de récupération de compte. L'authentification unique ne peut pas être activée sur votre instance tant qu'au moins un compte n'est pas configuré. Pour obtenir des détails sur ce processus, consultez Configurer un utilisateur de récupération de compte à partir de la page Propriétés de récupération de compte.

Remarque :
Si vous mettez à niveau une instance qui utilise déjà l'authentification unique ou Rome une version ultérieure, l'authentification unique continue de fonctionner sans qu'un utilisateur de récupération soit configuré.

Configuration de la récupération du compte

La fonctionnalité de récupération de compte est incluse dans les **modules d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).** La fonctionnalité est activée par défaut. Vous pouvez modifier ce paramètre ainsi que d'autres paramètres de récupération de compte à l'aide des propriétés système. Pour plus d'informations sur ces propriétés, reportez-vous à la section Propriétés de récupération de compte.

Contexte de la politique de récupération de compte

Une fois que vous avez enregistré un utilisateur de récupération de compte et activé l'authentification unique (SSO), votre instance restreint toutes les connexions locales. Cette restriction est définie dans le contexte de la politique **d'authentification SSO : contexte ACR** . Pour plus d'informations sur le contexte, reportez-vous à la section Contexte de récupération du compte.

Pour en savoir plus sur le fonctionnement des stratégies d'authentification et des contextes de politique sur votre instance, reportez-vous à la section Authentification adaptative.

Configurer un utilisateur de récupération de compte

Configurez un utilisateur de récupération de compte pour effectuer des activités de récupération de compte sur votre instance.

Un utilisateur de récupération de compte est un compte utilisateur que les administrateurs peuvent utiliser pour effectuer des tâches de récupération de compte, telles que le traitement d'une erreur de configuration SSO ou le traitement de certificats expirés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous utilisez la récupération de compte sur votre instance, vous devez configurer un utilisateur de récupération de compte. Cette étape est nécessaire avant d'activer l'authentification unique de plusieurs fournisseurs sur une instance.

Configurer un utilisateur de récupération de compte à partir de la page Propriétés de récupération de compte

Configurez une récupération de compte à partir de la page des propriétés de récupération de compte.

Avant de commencer
Rôle requis : admin

Pour qu'une nouvelle instance configure ACR, procédez comme suit :

- Activez le module d'extension Authentification unique (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled) : cette option est activée par défaut en cas d'instance nouvelle.
- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.
- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer la MFA avant de s'inscrire en tant qu'utilisateur ACR.

Pour qu'une instance mise à niveau utilise ACR, vous devez procéder comme suit :

- Activez le module d'extension Authentification unique (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled)

  Remarque :
  En cas d'instance mise à niveau, l'administrateur doit activer ACR.

- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.

  Remarque :
  Définir cette propriété sur faux ne désactive pas l'authentification unique (SSO) de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, l'ACR doit également être désactivé à l'aide de la `glide.sso.acr.enabled` propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.

- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer la MFA avant de s'inscrire en tant qu'utilisateur ACR.

Procédure

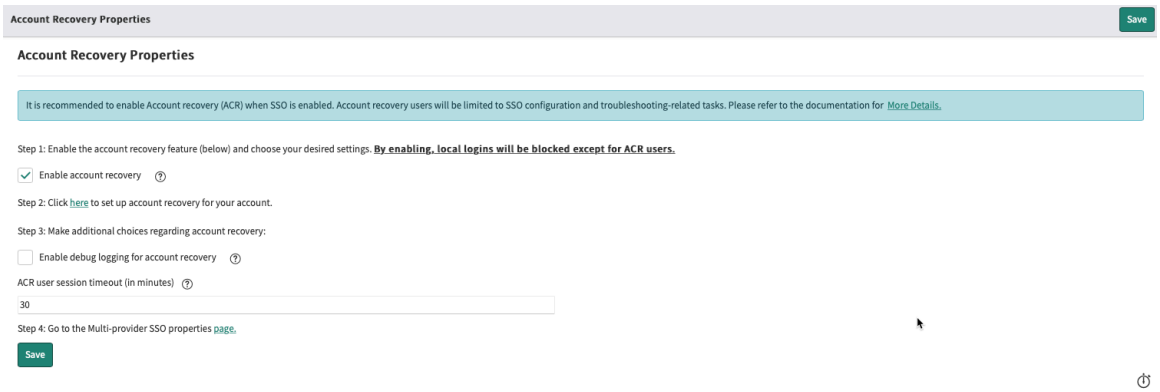
1. Accédez à la **Tous** > **Récupération de compte** > **Propriétés**.
2. Cliquez sur **Activer la récupération de compte**.

   Remarque :
   Vous devez activer la récupération de compte lorsque la SSO est activée. Les utilisateurs de récupération de compte sont limités à la configuration SSO et aux tâches liées au dépannage.

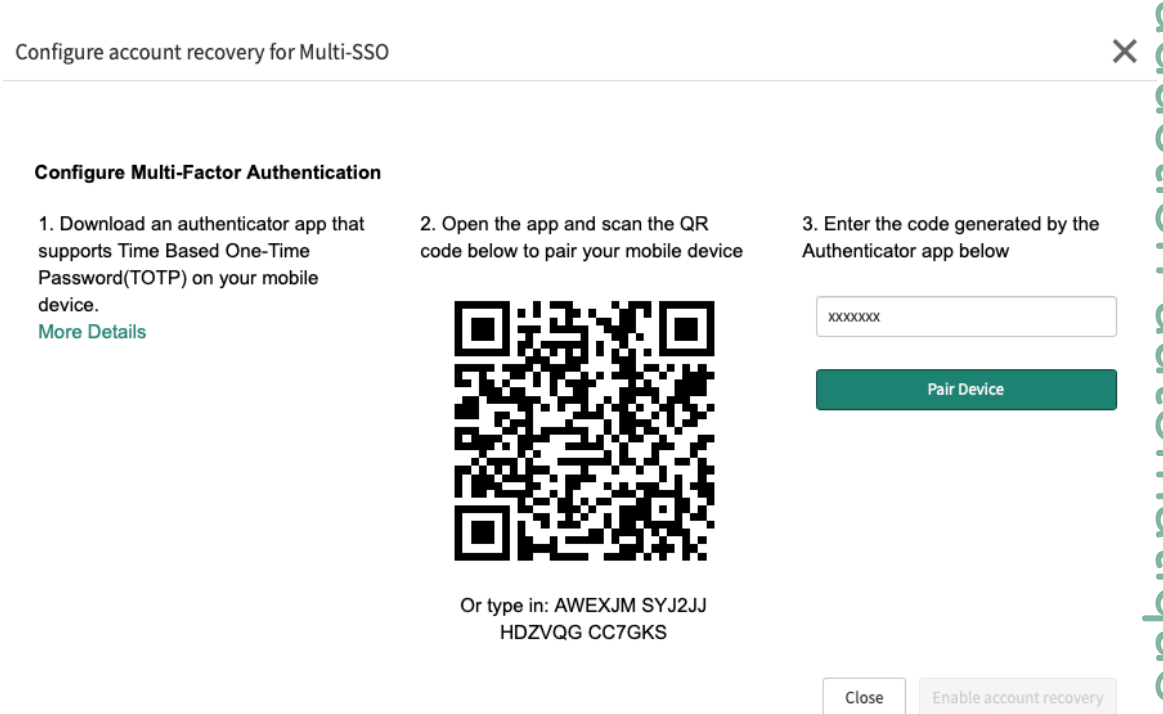
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur le texte **ici** à l'étape 2.



4. En suivant les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) multiple.**



Une fois les étapes affichées à l'écran terminées, l'option **Activer la récupération de compte** est activée.

5. Cliquez sur **Activer la récupération de compte**.

Résultats

Vous avez configuré votre compte d'utilisateur en tant qu'utilisateur de récupération de compte. Vous pouvez vérifier ce compte et voir tous les autres utilisateurs de récupération de compte configurés en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Utilisateurs**.

Configurer un utilisateur de récupération de compte à partir d'un profil d'utilisateur administrateur

Configurez un administrateur en tant qu'utilisateur de récupération de compte à partir du profil d'utilisateur administrateur.

Traduction automatique

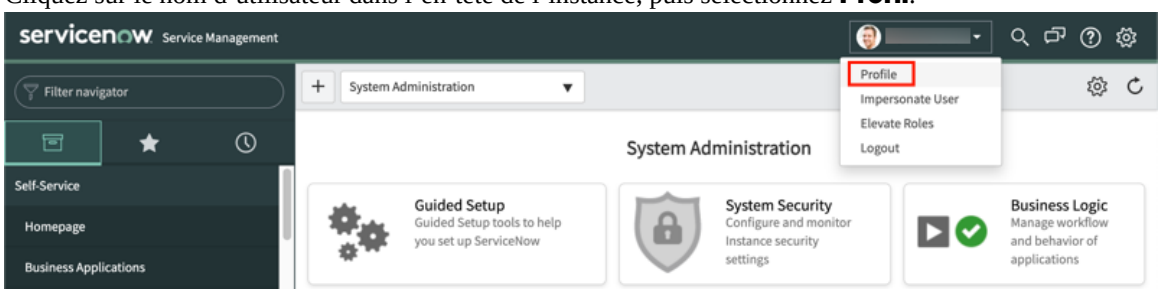
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

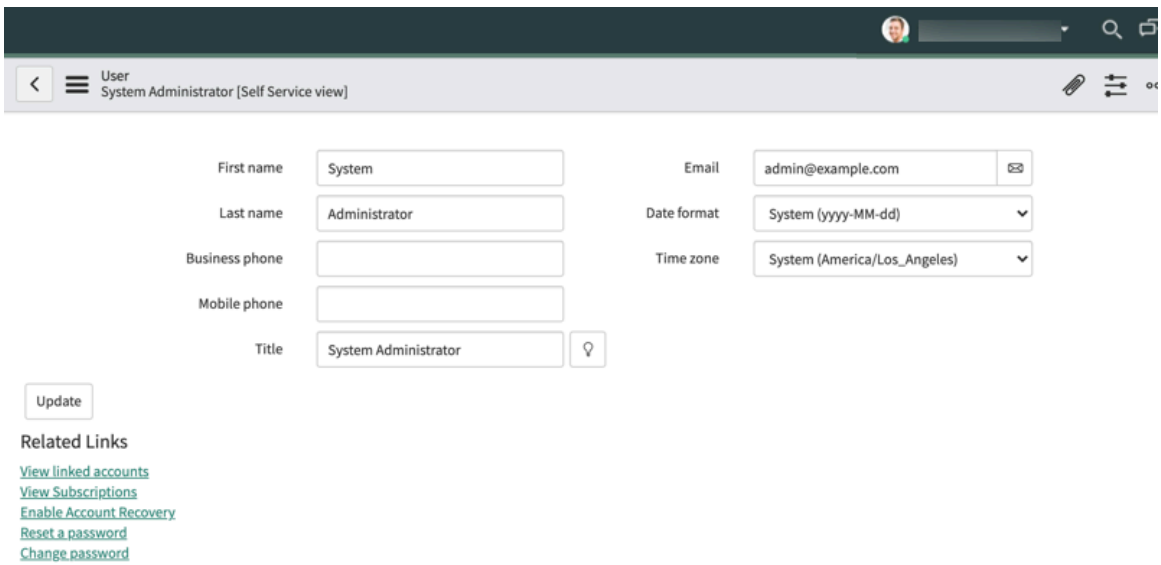
Rôle requis : admin

Procédure

1. Connectez-vous à votre instance à l'aide d'un compte administrateur.
2. Cliquez sur le nom d'utilisateur dans l'en-tête de l'instance, puis sélectionnez **Profil**.



3. Dans le formulaire **Utilisateur** , cliquez sur **Activer la récupération de compte** dans la section **Liens connexes** .



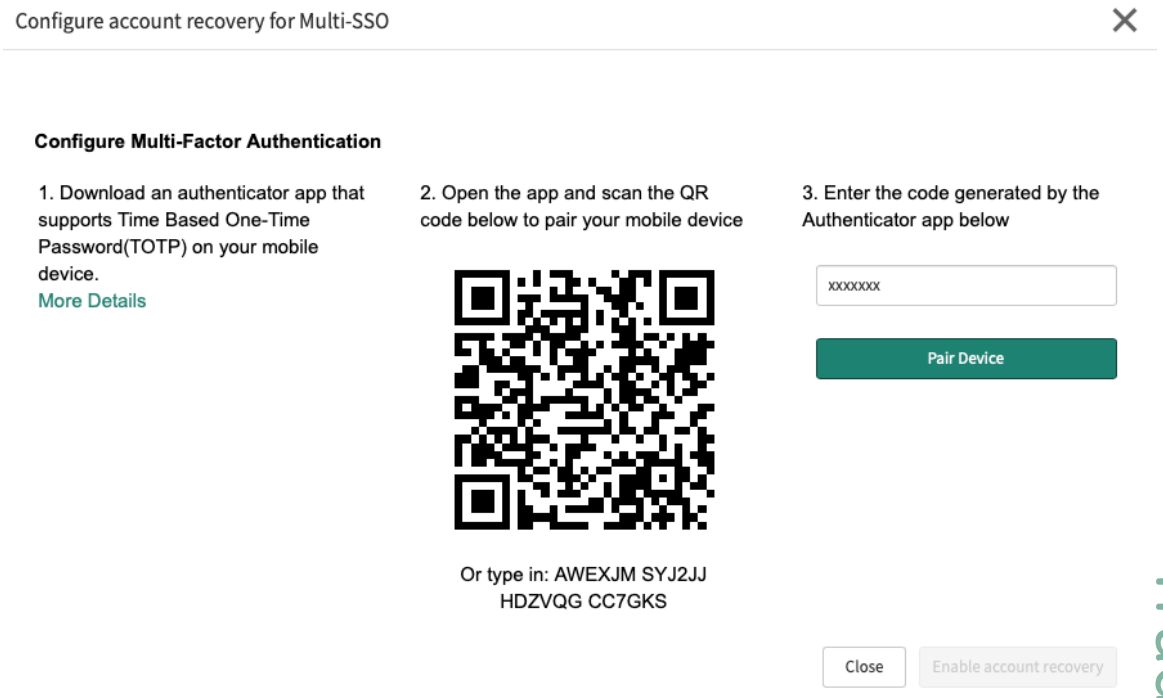
Remarque :

Si la récupération de compte est déjà activée pour l'utilisateur sélectionné, **l'option Activer la récupération de compte** n'apparaît pas dans les liens connexes. Il y aura une option **Désactiver la récupération de compte** à la place.

4. En suivant les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) multiple.**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois les étapes affichées à l'écran terminées, l'option **Activer la récupération de compte** est activée.

5. Cliquez sur **Activer la récupération de compte**.

Résultats

Vous avez configuré votre compte d'utilisateur en tant qu'utilisateur de récupération de compte. Vous pouvez vérifier ce compte et voir tous les autres utilisateurs de récupération de compte configurés en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Utilisateurs**.

Propriétés de récupération de compte

Utilisez les propriétés système pour configurer la récupération du compte (ACR) sur votre instance.

Accédez aux propriétés de récupération de compte sur votre instance en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Propriétés**.

Propriétés système de récupération de compte

Propriété	Description
Activer la fonctionnalité de récupération de compte [glide.sso.acr.enabled]	Indique si la fonctionnalité de récupération de compte est activée sur votre instance. Cette propriété est activée par défaut.
Activer la journalisation du débogage pour la récupération du compte [glide.sso.acr.debug.log.enabled]	Si votre instance inclut des informations de récupération de compte dans la journalisation de débogage. Cette propriété est désactivée par défaut.
Délai d'expiration de session utilisateur ACR (en minutes) [glide.sso.acr.ui.session.timeout]	Minutes d'inactivité avant que votre instance ne mette fin à une session utilisateur de récupération de compte. La valeur par défaut de cette propriété est de 30.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signature électronique pour l'authentification unique (SSO) de plusieurs fournisseurs

La signature électronique avec authentification unique (SSO) de plusieurs fournisseurs vous permet d'utiliser les propriétés de signature électronique à la place des propriétés SAML ou OIDC pour l'authentification.

Pour la vérification Single Sign-on (SSO) pendant l'authentification et pour exiger des utilisateurs qu'ils fournissent leurs informations d'identification avant de soumettre leur signature électronique, vous pouvez configurer l'authentification pour demander des informations d'identification à l'utilisateur avant de soumettre une signature.

Vous pouvez installer le module d'extension Approbations avec signature électronique (com.glide.e_signature_approvals) pour avoir la configuration de signature électronique pour les connexions SSO.

Remarque :
Vous devez installer Code Signing Signatures (com.glide.code_signing.signatures) pour installer le module d'extension Signature électronique.

Activer le module d'extension Approbation avec signature électronique

Le module d'extension Approval with e-Signature (com.glide.e_signature_approvals) permet aux utilisateurs d'approuver les demandes en saisissant à nouveau leurs informations d'identification de connexion.

Avant de commencer

Rôle requis : admin

Remarque :
Vous devez installer Code Signing Signatures (com.glide.code_signing.signatures) pour installer le module d'extension Signature électronique.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Utiliser l'authentification unique (SSO) de plusieurs fournisseurs pour configurer une approbation SSO pour une authentification SAML 2.0

Une approbation SSO avec signature électronique nécessite une configuration sur l'IdP SAML et l'instance ServiceNow .

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'IdP SAML doit prendre en charge et respecter l'attribut forceAuthn dans les demandes d'assertion SAML. La signature électronique ne fonctionne pas sans ce paramètre IdP. Configurez une approbation avec signature électronique à l'aide des informations d'identification d'une authentification SAML 2.0.

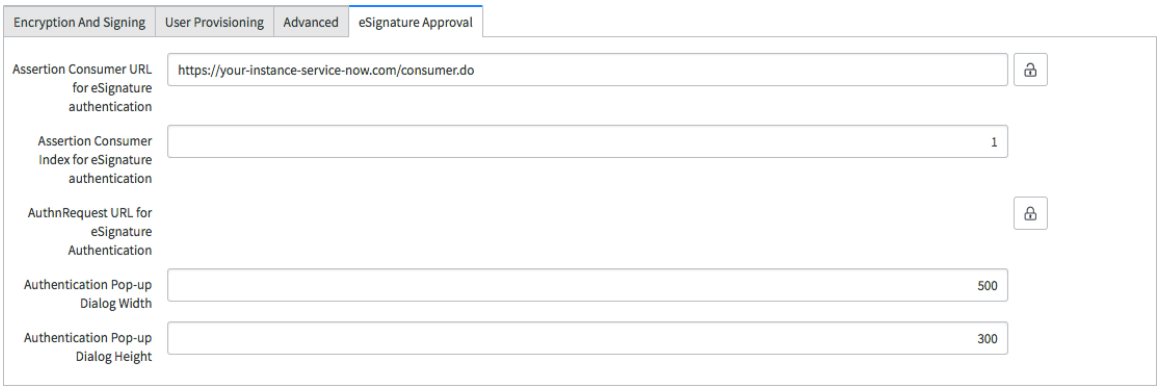
Procédure

1. Activez ou effectuez une mise à niveau vers SAML 2.0 à l'aide du module d'extension Activer l'authentification unique (SSO) de plusieurs fournisseurs.
2. Activez le module d'extension Approbation avec signature électronique.
3. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** et vérifiez votre configuration IdP SAML 2.0 L'onglet avancé affiche l'attribut **Forcer l'AuthnRequest** coché.
   Votre IdP SAML 2.0 doit prendre en charge l'attribut **Force AuthnRequest** , sinon la signature électronique n'est pas prise en charge.
4. Dans l'onglet Approbation de signature électronique, saisissez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété utilise par défaut l'URL appropriée. Pour configurer cette propriété, sélectionnez l'icône de verrou afin de rendre ce champ modifiable. Après les modifications, sélectionnez l'icône pour verrouiller le champ.
Index de consommateur d'assertion pour l'authentification de signature électronique	Si votre fournisseur de service dispose de plusieurs URL définies pour AssertionConsumerURL, vous pouvez définir l'index à utiliser pour les signatures électroniques, en commençant par l'index 1 ou plus.
URL AuthnRequest pour l'authentification de signature électronique	Vous pouvez entrer l'URL qui pointe vers l'URL SAML 2.0 IdP AuthnRequest pour l'authentification de signature électronique. Si l'URL est la même que l'URL de consommateur d'assertion, vous pouvez ne pas renseigner ce paramètre.
Largeur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir ses informations d'identification. Ce paramètre contrôle la largeur de cette boîte de dialogue. La valeur par défaut est 500.
Hauteur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir ses informations d'identification. Ce paramètre contrôle la hauteur de cette boîte de dialogue. La valeur par défaut est 300.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez le bouton **Générer les métadonnées** sous les onglets pour régénérer les métadonnées du fournisseur de service.
6. Copiez les métadonnées du fournisseur de service et mettez-les à jour sur l'IdP SAML.

Utiliser l'authentification unique (SSO) de plusieurs fournisseurs pour configurer une approbation SSO pour une authentification OIDC

Une approbation SSO avec signature électronique nécessite une configuration sur l'IdP SAML et l'instance ServiceNow .

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'IdP SAML doit prendre en charge et respecter l'attribut forceAuthn dans les demandes d'assertion SAML. La signature électronique ne fonctionne pas sans ce paramètre IdP. Configurez une approbation avec signature électronique à l'aide des informations d'identification d'une authentification SAML 2.0.

Procédure

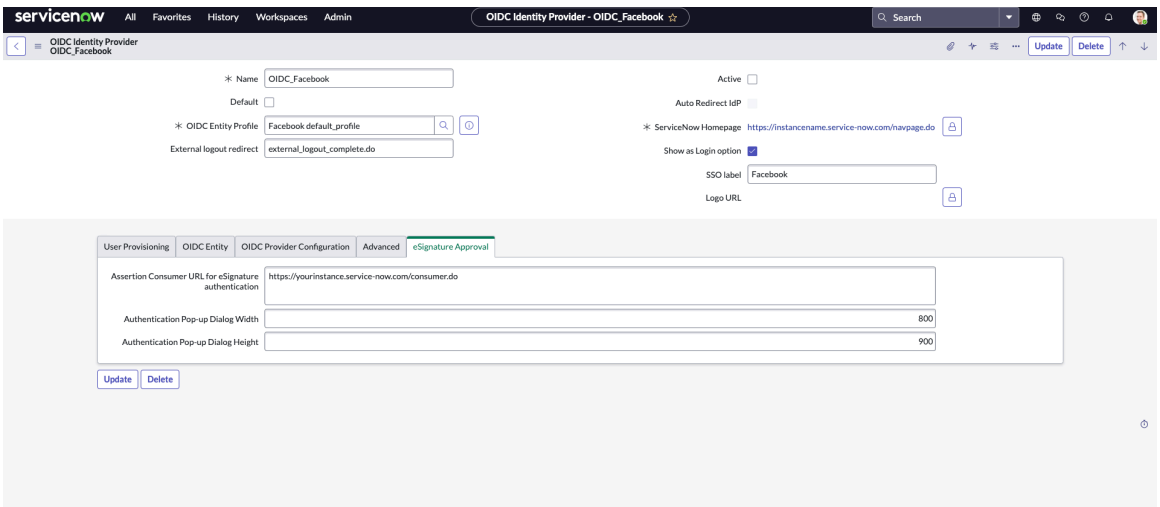
1. Activez le module d'extension Approbation avec signature électronique.
2. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** et vérifiez les configurations de votre fournisseur OIDC
3. Dans l'onglet Approbation de signature électronique, saisissez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété utilise par défaut l'URL appropriée. Pour configurer cette propriété, sélectionnez l'icône de verrou afin de rendre ce champ modifiable. Après les modifications, sélectionnez l'icône pour verrouiller le champ.
Largeur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir ses informations d'identification. Ce paramètre contrôle la largeur de cette boîte de dialogue. La valeur par défaut est 800.
Hauteur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir ses informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	d’identification. Ce paramètre contrôle la hauteur de cette boîte de dialogue. La valeur par défaut est 900.



4. Sélectionnez **Soumettre** si vous configurez la signature électronique lors de la configuration initiale OIDC ou **Mettre à jour** si vous souhaitez mettre à jour les détails de la signature électronique.

OpenID Connect (OIDC) en tant que fournisseur d’identité IdP (Single Sign-On)

OpenID Connect (OIDC) est une couche d’identité construite sur le protocole OAuth, qui vous offre, à vous et à vos utilisateurs finaux, une expérience d’authentification unique (SSO) moderne et intuitive.

OIDC améliore l’expérience de connexion pour les applications mobiles en permettant aux utilisateurs de se connecter aux ServiceNow applications à l’aide de leur fournisseur d’identité sociale. Par exemple, les administrateurs peuvent configurer l’authentification unique avec un fournisseur d’identité tiers qui prend en charge OpenID Connect. Les utilisateurs ont ensuite la possibilité de se connecter à votre application personnalisée ServiceNow à l’aide des informations d’identification de leur fournisseur d’identité.

Vous pouvez choisir d’utiliser des fournisseurs d’identité sociale tels que Google pour vos utilisateurs B2C (Business-to-Customer) et des fournisseurs d’identité d’entreprise tels que Okta, Microsoft Entra ID pour vos utilisateurs interentreprises.

Créer une configuration OpenID Connect (OIDC) pour l’authentification unique (SSO)

Créez ou mettez à jour une configuration OpenID Connect (OIDC) à l’aide du module d’extension SSO de plusieurs fournisseurs.

Configuration d’OpenID Connect (OIDC) pour Single Sign-On (SSO)

Avant de commencer

- Enregistrez une application OIDC auprès de votre fournisseur d’identité (IdP) et notez l’ID client, le secret client et l’URL de configuration connue.
- Activez le module d’extension SSO de plusieurs fournisseurs. La fonctionnalité SSO de plusieurs fournisseurs prend en charge la séparation de domaine. Vous pouvez spécifier différents IdP pour différents domaines.
- Configurer les propriétés SSO de plusieurs fournisseurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le module d'extension Approbation avec signature électronique pour activer la signature électronique pour l'IdP OIDC.
- Rôle requis : admin

Si vous disposez d'un ID client, d'un secret client et d'une URL de configuration connue du fournisseur d'identité, vous pouvez importer directement la configuration OIDC pour SSO.

Remarque :

- Le bouton **Connexion avec OIDC** ne s'affiche pas sur la page de connexion pour les fournisseurs d'identités basés sur OIDC si le module d'extension Séparation de domaine est installé.
- L'administrateur peut utiliser l'IdP basé sur OIDC pour activer SSO pour un utilisateur d'une entreprise ou d'un domaine spécifique.

Si vous ne disposez pas des informations requises sur le fournisseur d'identité, vous pouvez configurer manuellement OIDC pour SSO. Une fois la configuration terminée, les utilisateurs peuvent se connecter aux ServiceNow applications à l'aide de fournisseurs d'identité sociale tiers tels que Google Okta.

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Choisissez une des options suivantes.
   - Pour mettre à jour une configuration existante, cliquez sur un enregistrement de fournisseur d'identité OIDC.
   - Pour créer une configuration, cliquez sur **Nouveau** et sélectionnez **OpenID Connect**.
3. Pour une nouvelle configuration, entrez les informations de configuration OIDC de l'une des méthodes suivantes.

Option	Description
Importer la configuration connue OpenID Connect	Si vous disposez de l'URL de configuration connue ainsi que des informations d'identification de votre client associées, vous pouvez importer directement une configuration OIDC. **Remarque :** Si vous importez la configuration bien connue OIDC, tous les champs connexes sont renseignés automatiquement.
Configurer manuellement le formulaire Fournisseur d'identité OIDC	Si vous n'avez pas d'entité OAuth OIDC existante, fermez la fenêtre contextuelle Importer la configuration connue OpenID Connect et remplissez manuellement les champs du formulaire Fournisseur d'identité OIDC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer les champs de configuration connue OpenID Connect

Propriété	Description
Nom	Nom unique pour la configuration du fournisseur d'identité OIDC.
ID client	ID client de l'application enregistré dans le fournisseur d'identité OIDC tiers.
Secret client	Secret client de l'application enregistrée dans le fournisseur d'identité OIDC tiers.
URL de configuration reconnue	URL qui contient des métadonnées sur le fournisseur d'identité OIDC tiers.

Tous les champs obligatoires doivent être renseignés sur le formulaire Fournisseur d'identité OIDC.

Avant de remplir manuellement le formulaire Fournisseur d'identité OIDC, assurez-vous que vous disposez déjà d'un profil d'entité OAuth pour l'IdP OIDC.

Si vous n'avez pas de profil d'entité OAuth, vous pouvez le créer à l'aide des modèles de fournisseur OIDC externe par défaut, tels qu'Okta, Azure et d'autres.

Le type d'octroi du profil d'entité OAuth doit être accompagné d'un code d'autorisation. Pour plus d'informations, consultez Configurer un fournisseur OIDC OAuth sur le ServiceNow AI Platform.

Remarque :
Vous pouvez utiliser les modèles des fournisseurs d'identité tiers, Auth0, Azure AD, Google et Okta sont disponibles dans les données de démonstration du module d'extension Programme d'installation de l'authentification unique de plusieurs fournisseurs.

Champs Fournisseur d'identité OIDC

Propriété	Description
Nom	Nom de l'enregistrement du fournisseur d'identité OIDC.
Actif	Option permettant d'activer la configuration IdP OIDC. **Remarque :** Cette option ne peut être définie sur active qu'après un test de connexion réussi.
Par défaut	Option permettant de définir la configuration IdP OIDC par défaut lorsqu'il existe plusieurs configurations OIDC.
Rediriger automatiquement l'IdP	Option permettant d'activer la redirection automatique des utilisateurs vers la page de connexion du fournisseur d'identité. Ce champ s'affiche lorsque l'option **Définir comme IdP de redirection automatique** est définie sous la section Liens connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie se met automatiquement à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système contrôle cette fonctionnalité.
Profil de l'entité OIDC	Profil de l'entité OAuth pour la configuration OIDC.
ServiceNow Page d'accueil	URL de la page de connexion utilisée pour l'authentification. Ce champ est automatiquement défini sur l'URL de votre instance. Le format de l'URL est le suivant : https://yourinstance.service-now.com/navpage.do
Redirection de déconnexion externe	URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion. En règle générale, le portail, qui est utilisé pour la SSO. Ce champ est automatiquement défini sur external_logout_complete.do Par exemple, https://yourinstance.service-now.com/external_logout_complete.do
Afficher comme option de connexion	Option permettant d'afficher l'IdP OIDC comme option de connexion sur la page de connexion. L'option de connexion s'affiche sous la forme du bouton **Connexion avec fournisseur d'identité** .
Étiquette SSO	Étiquette de l'IdP OIDC affichée sur la page de connexion. Ce champ s'affiche uniquement lorsque **l'option Afficher comme connexion** est activée.
URL du logo	URL accessible au public qui contient le logo du fournisseur d'IdP OIDC. Ce champ s'affiche uniquement lorsque **l'option Afficher comme connexion** est activée.

4. **Facultatif :** Activez l'attribution automatique d'utilisateurs dans l'onglet Attribution d'utilisateurs>onglet Attribution d'utilisateurs.

(Optional) Vous pouvez choisir d'activer la mise en service automatique de l'utilisateur pendant la connexion de l'utilisateur. Lorsque la mise en service automatique d'un utilisateur est activée, un enregistrement utilisateur est automatiquement créé dans l'instance ServiceNow si cet enregistrement utilisateur n'existe pas.

Champs d'attribution d'utilisateurs

Propriété	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer la mise en service automatique d'un utilisateur. Cette propriété crée un utilisateur dans la table Utilisateur d'instance (sys_user) lorsque l'utilisateur quitte sur IdP, mais n'existe pas dans la table Utilisateur.
Mise en service à l'aide de	Source de données à utiliser pour transformer un jeton d'ID, un point de terminaison d'informations utilisateur ou à la fois un jeton d'ID et des informations utilisateur en utilisateur ServiceNow. Utilisez la liste de recherche pour sélectionner le modèle de source de données prédéfini, puis ouvrez l'enregistrement pour configurer le mappage de la table des transformations.
Mettre en service la source de données	Source de données de jeton d'ID utilisée pour l'attribution d'utilisateurs.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Source d'informations de l'utilisateur	Source de données du point de terminaison d'informations utilisateur utilisée pour l'attribution d'utilisateurs. Ce champ s'affiche lorsque les informations utilisateur ou le jeton d'ID et les informations utilisateur sont sélectionnés pour le champ **Mettre en service à l'aide** .
Mettre à jour l'utilisateur lors de la prochaine connexion	Option permettant d'activer la mise à jour de l'utilisateur lors de la prochaine connexion.
Mettre à jour la durée de l'intervalle d'utilisateur (en secondes)	Intervalle de temps minimum, en secondes, pour mettre à jour un enregistrement utilisateur entre les connexions suivantes. Ce champ est automatiquement défini sur 3 600 secondes. Par exemple, après la connexion d'un utilisateur, l'enregistrement utilisateur est mis à jour après 3 600 secondes jusqu'à la prochaine connexion. Ce champ n'est disponible que lorsque le champ **Mettre à jour l'utilisateur lors de la prochaine connexion** est activé.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Liste des rôles appliqués aux utilisateurs nouvellement mis en service.

5. Onglet Entité OIDC
   Vous pouvez afficher et modifier la configuration du client OIDC et le flux de connexion OIDC à l'aide de l'enregistrement d'entité.
6. Onglet Configuration du fournisseur OIDC
   Vous pouvez afficher et modifier l'URL de configuration connue de l'IdP OIDC ou de la validation de la demande de jeton d'ID.
7. **Facultatif :** Onglet Avancé

   (Optional) Scripts exécutés pendant l'authentification unique et la déconnexion.

   Champs avancés

Propriété	Description
Script d'authentification unique	Script qui s'exécute pendant l'authentification unique. Ce champ est automatiquement défini sur MultiSSO_OIDC_custom.
Script de déconnexion	Script qui s'exécute après la déconnexion de l'utilisateur. Ce champ est automatiquement défini sur MultiSSO_OIDC_logout_custom.

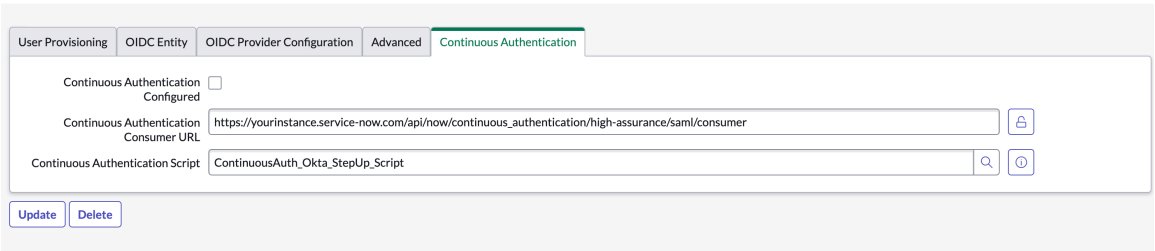
8. **Facultatif :** Dans l'onglet Authentification continue, configurez les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- L'onglet Authentification continue s'affiche uniquement lorsque vous installez le module d'extension **Authentification Zero Trust - continue** (com.snc.zero_trust_continuous_authentication) qui nécessite une licence.
- Si vous utilisez la stratégie d'authentification continue pour protéger l'accès à la table ou à la classe de données, reportez-vous à la section Authentification continue (CA).



Authentification continue

Champ	Description
Authentification continue configurée	Cochez la case pour activer la configuration.
URL du consommateur de l'authentification continue	Fournissez l'URL du consommateur à partir du fournisseur d'identité.
Script d'authentification continue	(Optional) Sélectionnez l'icône de recherche pour choisir le script fourni dans la plateforme. Dans cette configuration, pour OIDC Okta : **ContinuousAuth_Okta_StepUp_Script**

9. **Facultatif :** Dans l'onglet Approbation de signature électronique, configurez la signature électronique pour l'IdP OIDC.

Remarque :
L'onglet Approbation de signature électronique s'affiche uniquement lorsque vous installez le module **d'extension Approbation avec signature électronique** (com.glide.e_signature_approvals).

Champs d'approbation de signature électronique

Propriété	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Si vous utilisez une méthode personnalisée de gestion de l'authentification OIDC pour les signatures électroniques, vous pouvez configurer votre propre URL de consommateur. Par exemple, si vous utilisez l'authentification unique (SSO) de plusieurs fournisseurs, vous n'avez pas besoin d'utiliser cette propriété. Ce format d'URL est https://yourinstance.service-now.com/consumer.do

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Largeur de la boîte de dialogue contextuelle d'authentification	Largeur de la boîte de dialogue contextuelle d'authentification. Ce champ est automatiquement défini sur 800.
Hauteur de la boîte de dialogue contextuelle d'authentification	Hauteur de la boîte de dialogue contextuelle d'authentification. Ce champ est automatiquement défini sur 900.

10. **Facultatif :** Accédez à la page de connexion de l'instance pour vérifier que l'IdP apparaît comme option de connexion.
L'URL doit être au format suivant : https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

> **Remarque :**
> Si vous avez activé **l'option Sélectionné comme option de connexion**, vous pouvez accéder à l'URL de connexion de l'instance.

Utiliser l'authentification unique (SSO) basée sur Facebook

Connectez-vous à votre ServiceNow instance à l'aide de vos Facebook informations d'identification sur l'authentification unique basée sur Facebook.

Avant de commencer

L'authentification unique (SSO) basée sur Facebook est fournie avec votre ServiceNow instance.

Vous pouvez définir les configurations du fournisseur d'identité (IdP) pour l'IdP **OIDC_Facebook** en tant que **fournisseurs d'identité**. Pour plus d'informations sur les configurations IdP, reportez-vous à la section Configurer une authentification unique (SSO) basée sur Facebook.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sélectionnez **OIDC_Facebook**.
3. Sur la page OIDC_Facebook, spécifiez les champs suivants :

> **Remarque :**
> - La plupart des champs sont renseignés automatiquement lors de l'utilisation de l'IdP par défaut.
> - Les détails de la ServiceNow page d'accueil doivent être fournis.
> - Les détails relatifs à l'utilisateur, tels que l'ID client et le secret client, Facebook doivent être fournis dans l'IdP.

OIDC_Facebook les détails du fournisseur d'identité

Champ	Description
Nom	Nom de l'enregistrement IdP OIDC. Entrez OIDC_Facebook.

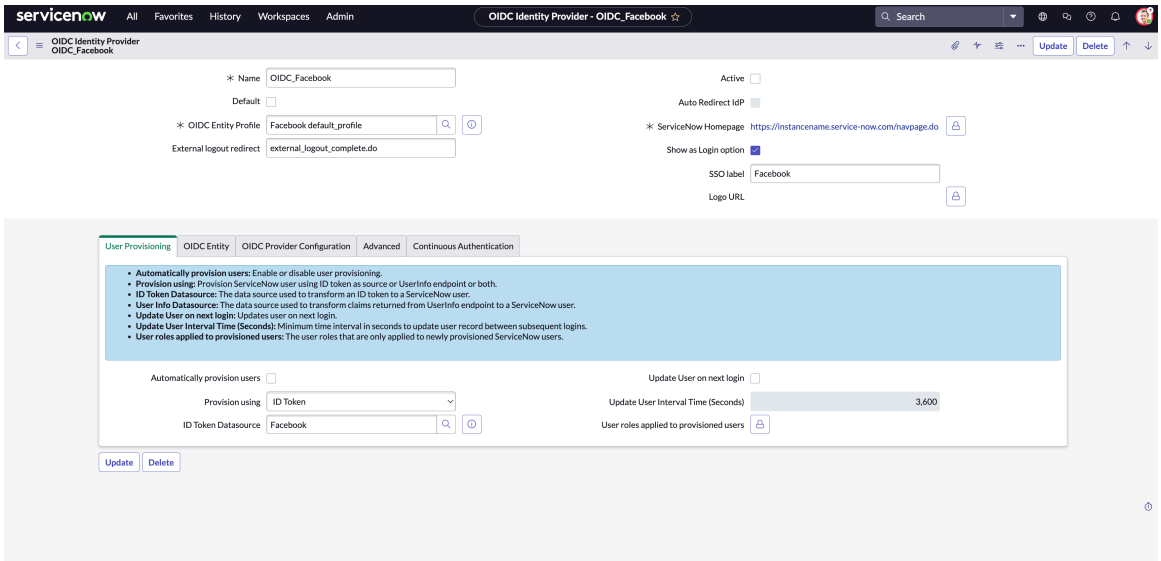
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Par défaut	Option permettant de définir la configuration IdP OIDC par défaut.
Profil de l'entité OIDC	Profil de l’entité OAuth pour la configuration OIDC. C’est là qu’intervient Facebook default_profile.
Redirection de déconnexion externe	URL vers laquelle l’intégration redirige les utilisateurs après leur déconnexion. En règle générale, cette URL correspond au portail utilisé pour SSO. Ce champ est automatiquement défini sur **external_logout_complete.do**. Par exemple, https://<votreinstance>.service-now.com/external_logout_complete.do.
Actif	Option permettant d’activer la configuration IdP OIDC. **Remarque :** Cette option ne peut être définie sur active qu’après un test de connexion réussi.
Rediriger automatiquement l'IdP	Option permettant d’activer la redirection automatique des utilisateurs vers la page de connexion du fournisseur d’identité.
ServiceNow Page d’accueil	URL de la page de connexion utilisée pour l’authentification. Ce champ est automatiquement défini sur l’URL de votre instance. Le format de l’URL est https://<votreinstance>.service-now.com/navpage.do
Afficher comme option de connexion	Option permettant d’afficher l’IdP OIDC comme option de connexion sur la page de connexion. Dans ce cas, l’option de connexion apparaît sous la forme **du bouton Connexion avec Facebook** .
Étiquette SSO	Étiquette de l’IdP OIDC affichée sur la page de connexion. Ce champ s’affiche uniquement lorsque **l’option Afficher comme connexion** est activée.
URL du logo	URL accessible au public qui contient le logo du fournisseur d’IdP OIDC. Ce champ s’affiche uniquement lorsque **l’option Afficher comme connexion** est activée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. **Facultatif :** Ouvrez l’onglet **Attribution d’utilisateurs** et renseignez les champs.

> **Remarque :**
> Vous devez configurer les informations relatives à OIDC telles que l’ID client et le secret client de vos utilisateurs à partir de Facebook.

Onglet Attribution d’utilisateurs

Champ	Description
Attribuer automatiquement les utilisateurs	Option permettant d’activer la mise en service automatique d’un utilisateur. Cette propriété crée un utilisateur dans la table Utilisateur [sys_user] de l’instance lorsque l’utilisateur existe sur l’IdP, mais n’existe pas dans la table Utilisateur. **Remarque :** Vous pouvez choisir d’activer la mise en service automatique de l’utilisateur pendant la connexion de l’utilisateur. Lorsque la mise en service automatique d’un utilisateur est activée, un enregistrement utilisateur est automatiquement créé dans l’instance ServiceNow si cet enregistrement utilisateur n’existe pas.
Mise en service à l'aide de	La source de données à utiliser pour la transformation en utilisateur ServiceNow . Les choix sont les suivants : ○ **Un jeton d’ID** ○ **Point de terminaison d’informations utilisateur** ○ **Jeton d'ID et informations utilisateur** Utilisez la liste de recherche pour sélectionner le modèle de source de données prédéfini, puis ouvrez l’enregistrement pour configurer le mappage de la table des transformations.
Mettre en service la source de données	Source de données de jeton d’ID utilisée pour la mise en service d’utilisateur.
Source d'informations de l'utilisateur	La source de données du point de terminaison d’informations utilisateur utilisée pour l’attribution d’utilisateurs. Ce champ **s’affiche** uniquement lorsque Informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	utilisateur ou **Jeton d'ID et Informations utilisateur** sont sélectionnés dans le champ **Mettre en service à l'aide** .
Mettre à jour l'utilisateur lors de la prochaine connexion	Option permettant d'activer les mises à jour de l'utilisateur lors de la prochaine connexion.
Mettre à jour la durée de l'intervalle d'utilisateur (en secondes)	Intervalle de temps minimal (en secondes) pour mettre à jour un enregistrement utilisateur entre les connexions suivantes. Ce champ est automatiquement défini sur 3 600 secondes. Par exemple, après la connexion d'un utilisateur, l'enregistrement utilisateur est mis à jour après 3 600 secondes jusqu'à la prochaine connexion. Ce champ n'est disponible que lorsque le champ **Mettre à jour l'utilisateur lors de la prochaine connexion** est activé.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Liste des rôles appliqués aux utilisateurs nouvellement mis en service.

5. Dans l'onglet **Entité OIDC** , affichez et modifiez la configuration du client OIDC et le flux de connexion OIDC à l'aide de l'enregistrement d'entité.
   Pour plus d'informations sur la configuration basée sur OIDC, consultez Configurer un fournisseur OIDC OAuth pour accepter les jetons tiers
6. Dans l'onglet **Configuration du fournisseur OIDC** , affichez et modifiez l'URL de configuration connue de l'IdP OIDC.
7. **Facultatif :** Ouvrez l'onglet **Avancé** et renseignez les champs.

Onglet Avancé

Propriété	Description
Script d'authentification unique	Script qui s'exécute pendant l'authentification unique.
Script de déconnexion	Script qui s'exécute après la déconnexion de l'utilisateur.

Remarque :
Les scripts sont exécutés pendant l'authentification unique et la déconnexion.

8. Pour activer et tester la configuration, cliquez sur **Actif**.
9. Pour mettre à jour l'enregistrement, cliquez sur **Mettre à jour**.
   L'option de connexion basée sur Facebook est affichée sur le formulaire de connexion.
10. Lorsque vous vous connectez sur le formulaire de connexion, procédez comme suit :
    a. Sélectionnez l'option Facebook .
    b. Pour vous connecter à l'instance ServiceNow , spécifiez vos Facebook informations d'identification.

Configurer une authentification unique (SSO) basée sur Facebook

Configurez une SSO basée sur Facebook pour votre ServiceNow instance.

Avant de commencer

Disposer d'un ID client valide configuré en tant qu'IdP à partir de Facebook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activez les propriétés suivantes :

- Activer l'authentification unique (SSO) de plusieurs fournisseurs.
- Activez la journalisation du débogage pour les intégrations SSO de plusieurs fournisseurs.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Pour créer un nouveau Facebook fournisseur d'identité, cliquez sur **Nouveau**.
3. Cliquez sur **OpenID Connect**.
4. Remplissez les champs du formulaire.

Importer le formulaire de configuration connue OpenID Connect

Champs	Description
Nom	Nom unique pour la configuration du fournisseur d'identité OIDC.
ID client	L'ID client de l'application enregistré dans le fournisseur d'identité OIDC tiers.
Secret client	Le secret client de l'application enregistré dans le fournisseur d'identité OIDC tiers.
URL de configuration reconnue	URL qui contient les métadonnées sur le fournisseur d'identité OIDC tiers.

5. Cliquez sur **Importer**.
   L'IdP basé sur Facebook est créé.
6. Sélectionnez l'IdP Facebook .
7. Dans l'idP Facebook , procédez comme suit :
   a. Validez tous les champs tels que **Nom**, **Profil de l'entité OIDC**, **Redirection de déconnexion externe** et **Page d'accueil ServiceNow**.
   b. Fournissez votre **étiquette SSO**.
8. Dans l'onglet **Attribution d'utilisateurs** , spécifiez les champs dont vous avez besoin pour configurer les utilisateurs pour une attribution d'utilisateurs et des rôles spécifiques.

   Seuls les champs obligatoires sont requis. Vous pouvez spécifier les champs restants en fonction de vos besoins.
9. Dans l'onglet **Entité OIDC** , procédez comme suit :
   a. Cliquez sur l'entité.
   b. Définissez le champ **URL de redirection** sur votre Facebook URL de redirection.
10. Dans l'onglet **Profils des entités OAuth** , procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans les détails du profil, cliquez sur un profil.

b. Sélectionnez un périmètre et vérifiez les détails.
Par exemple, sélectionnez **le champ d'application-1**

11. Dans l'onglet **Périmètres des entités OAuth** , cliquez sur le lien **Périmètre-1** et ajoutez le périmètre comme e-mail.
12. Pour enregistrer la configuration, cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer**.
13. Pour définir la configuration comme active, sélectionnez **Actif**.

Résultats

Les utilisateurs sont affichés avec l'option Facebook SSO sur le formulaire de connexion.

SAML

Le langage SAML (Security Assertion Markup Language) est une norme XML pour l'échange de données d'authentification et d'autorisation entre les domaines de sécurité.

SAML échange des informations de sécurité entre un fournisseur d'identité (un producteur d'assertions) et un fournisseur de service (un consommateur d'assertions). SAML est un produit du comité technique des services de sécurité OASIS. Lorsqu'il est correctement implémenté, SAML est l'une des méthodes d'authentification unique (SSO) les plus sécurisées disponibles.

L'intégration SAML 2.0 permet l'authentification unique en échangeant des jetons XML avec un fournisseur d'identité (IdP) externe. L'IdP authentifie l'utilisateur et transmet un jeton NameID au système. Si le système trouve un utilisateur avec un jeton NameID correspondant (par exemple, l'adresse e-mail), l'instance journalise cet utilisateur.

Si vous utilisez le module d'extension SAML 2.0 pour l'authentification SSO, vous devez définir la propriété glide.ui.rotate_sessions sur false. Sinon, cela interfère avec le partage d'informations de session qui a lieu entre l'instance et le fournisseur d'identité. Les utilisateurs disposant du privilège security_admin élevé peuvent accéder à cette propriété.

Remarque :
Il est recommandé aux clients utilisant une intégration SAML 2.0 existante d'effectuer une mise à niveau vers le module d'extension SSO de plusieurs fournisseurs.

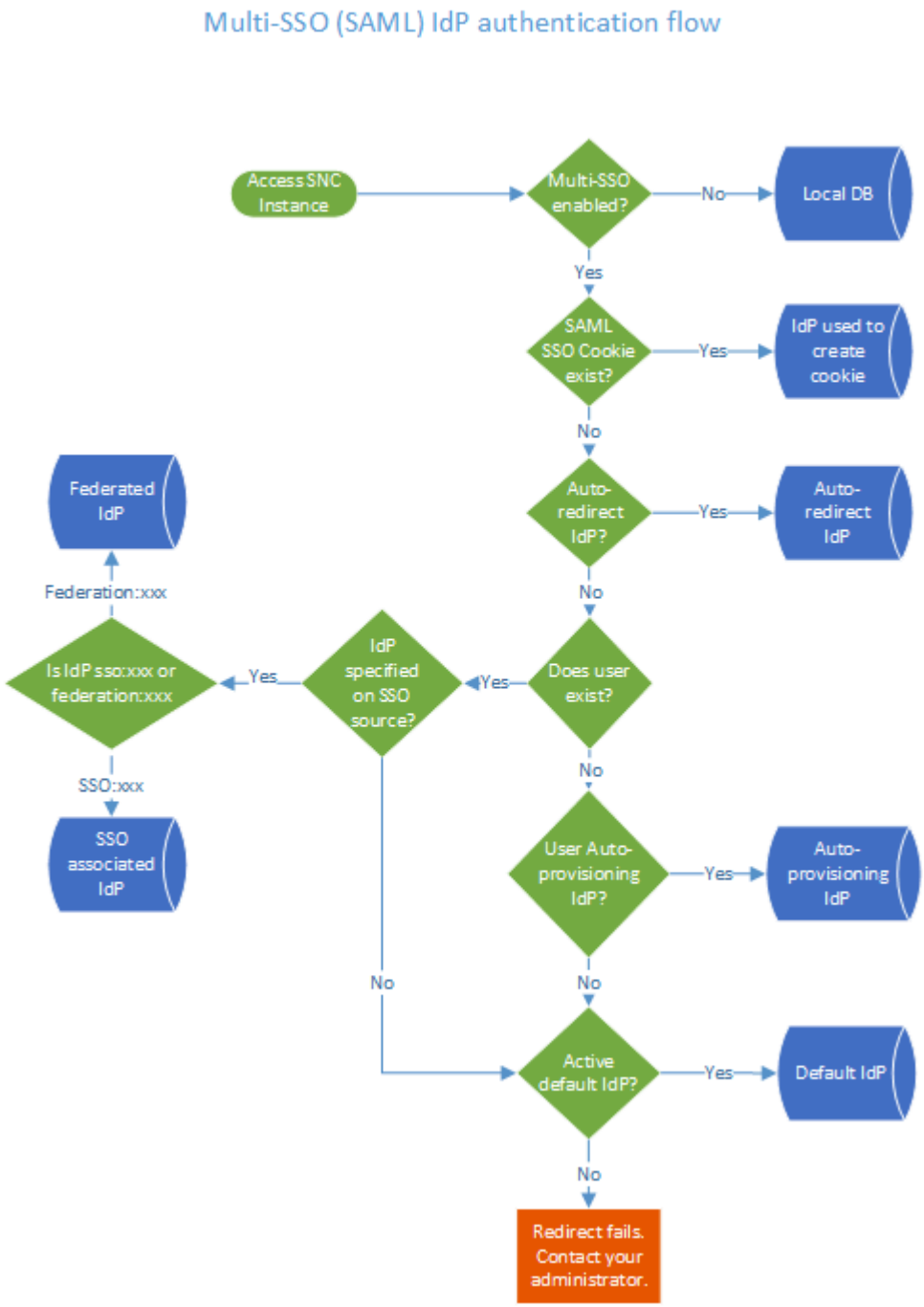
Flux d'authentification IdP SSO de plusieurs fournisseurs (SAML)

Décrit les différentes entités qui peuvent authentifier un utilisateur via le multi-SSO SAML.

Vous pouvez suivre le flux d'authentification pour comprendre quand une entité authentifie un utilisateur à l'aide de l'authentification unique (SSO) à l'aide de l'authentification unique (SSO).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Local DB

Si l'authentification unique (SSO) n'est pas activée, l'authentification dirige vers une base de données locale.

SAML SSO Cookie IdP

Si un cookie SSO SAML existe, l'IdP spécifié avec ce cookie authentifie l'utilisateur.

Rediriger automatiquement l'IdP

Si l'IdP de redirection automatique est activée, cet IdP authentifie l'utilisateur.

IdP fédéré

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion de l'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table utilisateur avec l'IdP défini dans le champ **Source SSO** en tant que fédération : xxx, l'IdP fédéré authentifie l'utilisateur.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

IdP associé

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion de l'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table utilisateur avec l'IdP défini dans le champ **Source SSO** comme sso : xxx, l'IdP associé authentifie l'utilisateur.

Mise en service automatique de l'IdP

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion de l'autorisation externe (login_locate_sso.do) et que l'utilisateur n'existe pas dans la table utilisateur, mais que la mise en service automatique est activée, l'IdP de mise en service automatique authentifie l'utilisateur.

Remarque :
S'il existe plusieurs IdP de mise en service automatique activés, l'utilisateur peut choisir celui de mise en service automatique qu'il peut utiliser.

IdP par défaut

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion à l'autorisation externe (login_locate_sso.do) et que l'utilisateur :

- N'existe pas dans la table utilisateur, la mise en service automatique n'est pas activée et il existe un IdP par défaut actif
- Existe dans la table utilisateur, un IdP n'est pas spécifié sur l'enregistrement de l'utilisateur source ou de la société SSO et il existe un IdP actif par défaut

l'IdP par défaut authentifie alors l'utilisateur.

Propriétés système du fournisseur d'identité (IdP)

Un IdP propose généralement un document XML contenant ses métadonnées d'authentification et de déconnexion.

Par exemple, SSOCircle publie ses métadonnées en ligne.

Parcourez les métadonnées IdP pour trouver les entrées suivantes :

- L'élément `SingleSignOnService` avec un attribut `Binding` qui contient une valeur de `HTTP-Redirect`. L'attribut `Location` répertorie l'URL requise par l'intégration pour le service AuthnRequest.
- L'élément `SingleLogoutService` avec un attribut `Binding` qui contient une valeur de `HTTP-Redirect`. L'attribut `Location` répertorie l'URL dont l'intégration a besoin pour le service SingleLogoutRequest.

Remarque :
L'intégration SAML 2.0 ne prend en charge que la liaison aux services IdP par HTTP-Redirect.

Par exemple :

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLocation="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

Définir l'URL de l'émetteur d'IdP

Fournissez l'URL aux fournisseurs d'identités qui émettront le jeton de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
L'intégration vérifie que chaque réponse SAML contient la même URL répertoriée dans cette propriété système que l'URL répertoriée dans l'élément *Émetteur* . Par exemple :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Procédure

1. Accédez à la **Tous** > **Authentification unique SAML 2** > **Propriétés**.
2. Dans la propriété *URL du fournisseur d'identité qui émettra le jeton de sécurité SAML2 avec les informations de l'utilisateur*, saisissez l'URL vers votre fournisseur d'identités.

   Chaque URL IdP doit être unique. Par défaut, l'intégration contient l'URL vers SSOCircle. Pour plus d'informations, consultez http://idp.ssocircle.com .

Définir l'URL du service AuthnRequest

À l'aide des métadonnées de l'IdP, définissez les URL de service de demandes pour l'IdP de l'intégration.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans la propriété *L'URL de base vers le service AuthnRequest du fournisseur d'identité. L'AuthnRequest sera publiée sur cette URL comme paramètre* SAMLRequest, entrez l'URL vers la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService .
2. Cochez la case à côté de *Signer la demande AuthnRequest* pour activer le service d'authentification unique du fournisseur d'identité pour recevoir une demande AuthnRequest signée.
3. Dans la propriété *Lorsque l'authentification unique SAML 2.0 échoue parce que la session n'est pas authentifiée ou s'il s'agit de la première connexion, redirigez vers cette URL. Il s'agit de l'URL de base vers laquelle la SAML 2.0 AuthnRequest initiale est envoyée à l'aide du paramètre* SAMLRequest, entrez l'URL vers la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService .

   Par défaut, l'intégration contient l'URL du service SSOCircle.

Définir l'URL du service SingleLogoutRequest

Définissez les URL du service de demande pour l'IdP de l'intégration à l'aide des métadonnées de l'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans l'URL *de base du service SingleLogoutRequest du fournisseur d'identité. La LogoutRequest sera publiée sur cette URL en tant que propriété de paramètre* SAMLRequest, entrez l'URL obtenue à partir de l'élément SingleLogoutService .
   La LogoutRequest est publiée sur cette URL comme paramètre SAMLRequest. Par défaut, l'intégration contient l'URL du service SSOCircle.
2. Dans *l'URL permettant de rediriger les utilisateurs après la déconnexion, généralement vers le portail qui a activé la propriété SSO (par exemple, http://portal.companya.com/logout)*, saisissez l'URL à partir de laquelle vous souhaitez rediriger les utilisateurs après leur déconnexion.

   Si votre fournisseur d'identité utilise l'authentification basée sur le formulaire, saisissez l'URL dans le formulaire de connexion de votre fournisseur d'identités. Si votre IdP utilise une méthode d'authentification non basée sur un formulaire telle que Kerberos, vous devez définir l'URL sur une page de déconnexion statique. De cette façon, les utilisateurs qui se déconnectent ne sont pas immédiatement redirigés vers l'IdP et se connectent à nouveau. Par défaut, l'intégration contient l'URL de la page d'interface utilisateur statique external_logout_complete.do.

(Facultatif) Activer les demandes de déconnexion signées

Certains fournisseurs d'identités exigent que le fournisseur de service signe les demandes de déconnexion avec un certificat.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Si votre fournisseur d'identités nécessite des demandes de déconnexion signées, utilisez les métadonnées du fournisseur d'identités pour définir les propriétés système suivantes.

Procédure

1. Dans l'onglet **Avancé** , à partir de la propriété *Sign LogoutRequest. Définissez cette propriété sur vrai si le service SingleLogoutRequest du fournisseur d'identité nécessite une LogoutRequest* signée, sélectionnez **Oui** pour spécifier que votre fournisseur d'identités requiert une demande de déconnexion signée ou sélectionnez **Non** pour utiliser des demandes de déconnexion non signées.
2. Si vous avez sélectionné **Oui** pour *signer LogoutRequest*, alors dans *Le protocole de liaison du service SingleLogoutRequest du fournisseur d'identité. (La valeur peut être « urn :oasis :names :tc :SAML :2.0 :bindings :HTTP-Redirect » ou « urn :oasis :names :tc :SAML :2.0 :bindings :HTTP-POST ».)* , entrez l'une des valeurs prises en charge répertoriées dans Attribut Liaison à partir de l'élément SingleLogoutService .

   Par défaut, l'intégration utilise une liaison HTTP-Redirect.
3. Cliquez sur **Mettre à jour**.
4. Installez un magasin de clés de fournisseur de service (SP).

Propriétés système du fournisseur de services (SP)

Ces propriétés système définissent la façon dont l'instance interagit avec l'IdP en tant que fournisseur de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivez le processus séquentiel pour définir l'IdP en tant que fournisseur de service.

Définir l'URL d'instance pour SAML

Définissez les URL spécifiques à l'instance afin que l'IdP puisse authentifier les utilisateurs.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans la propriété *URL de l'instance Service-now (généralement cette instance)*, saisissez l'URL (y compris la page de connexion) de l'instance pour laquelle l'IdP s'authentifie.
   Par exemple : https://yourinstance.service-now.com/navpage.do
2. Dans la propriété *L'identification d'entité ou l'émetteur*, saisissez l'URL de base (à l'exclusion de la page de connexion) de l'instance pour laquelle l'IdP s'authentifie.
   Par exemple : https://yourinstance.service-now.com/

Définir l'URL de l'audience pour SAML

Permettez à votre instance de vérifier qu'elle est bien le destinataire prévu d'une réponse SAML à l'aide de la propriété Audience.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
L'intégration vérifie que chaque réponse SAML contient la même URL répertoriée dans cette propriété système que l'URL répertoriée dans l'élément *Audience* . Par exemple :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
...
</samlp:Response>
```

Procédure

1. Accédez à la **Tous** > **Authentification unique SAML 2** > **Propriétés**.
2. Dans la propriété *L'URI du public qui accepte les jetons SAML2. (Il s'agit normalement de votre URI d'instance. Par exemple : https://<nom d'instance>.service-now.com.)*, saisissez l'URL de votre instance.
   Par exemple, https://demoi2.service-now.com. Cette URL doit correspondre à la valeur de l'élément *Audience* dans la réponse SAML.
3. Cliquez sur **Mettre à jour**.

Configurer une politique NameID pour SAML

Configurez une politique NameID pour SAML. SAML 2.0 exige que l'IdP échange un jeton NameID avec le fournisseur de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Pour l'intégration SAML 2.0, le jeton NameID doit être mappé à un champ particulier de la table Utilisateur. L'intégration utilise la valeur du jeton NameID pour déterminer l'utilisateur authentifié par l'IdP.

Procédure

1. Parcourez les métadonnées IdP pour trouver l'élément `NameIDFormat` qui contient une valeur `emailAddress`.
   La valeur de cet élément est le format par défaut utilisé par l'intégration.
2. Examinez d'autres éléments `NameIDFormat` pour déterminer s'il existe des formats qui correspondent à d'autres champs de la table Utilisateur.

Déterminer quel champ de table Utilisateur correspond au jeton NameID

Les fournisseurs d'identité spécifient le format du jeton `NameID` .

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La configuration de SAML 2.0 nécessite la sélection d'un champ dans la table Utilisateur qui correspond au format du jeton `NameID` . En règle générale, les fournisseurs d'identité offrent la possibilité d'utiliser une adresse e-mail comme jeton `NameID` . Étant donné que la table Utilisateur contient un champ d'e-mail, ce champ est un choix logique pour une utilisation en tant que jeton `NameID` . Pour utiliser un autre champ de la table Utilisateur comme jeton `NameID` , vérifiez d'abord que l'IdP offre un format `NameID` qui correspond à la valeur d'un champ de la table Utilisateur. Cela peut nécessiter l'ajout du champ à la table Utilisateur.

Procédure

1. Comparez les formats disponibles dans l'élément `NameIDFormat` de l'IdP aux champs de la table Utilisateur.
2. Sélectionnez un format `NameID` où il y a une valeur correspondante dans la table Utilisateur.
3. Dans le *champ Table utilisateur à associer à l'élément NameID de l'objet dans le champ SAMLResponse* , entrez le nom du champ Table Utilisateur pour rechercher les valeurs correspondantes dans le jeton `NameID` .

   Par défaut, l'intégration utilise le champ E-mail.

Définir la politique IdP NameID

Spécifiez le format que l'IdP utilise pour le jeton `NameID` .

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ce format est répertorié dans le cadre des métadonnées de l'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la propriété *La politique NameID à utiliser pour renvoyer le NameID de l'objet dans SAMLResponse. Votre fournisseur d'identité SAML devra prendre cela en charge en déclarant la politique dans ses métadonnées. La valeur NameID est utilisée pour correspondre au champ spécifié dans la table Utilisateur pour rechercher l'utilisateur.* Entrez la valeur de l'élément `NameIDFormat` que l'intégration utilise.

   Par défaut, l'intégration utilise SSOCircle `NameIDFormat` pour les adresses e-mail.

2. Cliquez sur **Enregistrer**.

Valeurs du champ Table d'utilisateur pour SAML

Assurez-vous que le champ Table d'utilisateur de l'intégration contient des valeurs correspondantes appropriées.

Par exemple, si l'intégration utilise le champ d'e-mail comme jeton `NameID` , assurez-vous que l'instance répertorie la même adresse e-mail que l'IdP. L'intégration échoue à authentifier les utilisateurs qui n'ont pas de valeur correspondante pour le jeton `NameID` .

(Facultatif) Activer la fourniture d'une classe de contexte d'authentification pour SAML

Vous pouvez activer l'instance pour envoyer une demande de classe de contexte d'authentification à l'IdP contenant le format de demande d'authentification préféré de votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Si vous activez la création d'un message AuthContextClass, vous devez également spécifier un format de référence de classe de contexte d'authentification.

Remarque :
Certains fournisseurs d'identités n'autorisent pas le fournisseur de service à définir la classe de contexte d'authentification. La désactivation de ce paramètre permet à l'IdP de choisir la classe de contexte d'authentification.

Procédure

1. À partir de la propriété *Créez une demande AuthnContextClass Dans l'instruction AuthnRequest*, sélectionnez **Oui** pour spécifier une classe de contexte particulière telle que Transport protégé par mot de passe, ou sélectionnez **Non** pour que l'IdP sélectionne la classe de contexte la plus appropriée.
2. Si vous avez sélectionné **Oui** pour *créer une demande AuthnContextClass dans la déclaration AuthnRequest*, dans la *méthode AuthnContextClassRef que nous demanderons dans notre propriété SAML 2.0 AuthnRequest to the Identity Provider* , saisissez l'URN de la classe de contexte que vous souhaitez utiliser pour l'authentification (voir table).

Options URN AuthnContextClass

Type d'authentification	Classe de contexte d'authentification URN
Authentification basée sur les formulaires	urn :oasis :names :tc :SAML :2.0 :ac :classes :PasswordProtectedTransport
Authentification basée sur Kerberos	urn :federation :authentication :windows

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, l'intégration utilise une méthode d'authentification de transport protégée par mot de passe.

3. Cliquez sur **Mettre à jour**.

(Facultatif) Définir les propriétés du magasin de clés pour signer les demandes de déconnexion pour SAML

Définissez les propriétés du magasin de clés pour permettre à l'intégration de signer les demandes de déconnexion à l'aide de votre serveur signé et des certificats de l'autorité de certification signés.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans la propriété *Alias de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, entrez le nom d'alias que vous avez créé pour le magasin de clés SAML 2.0.
   Par défaut, l'intégration recherche l'alias *saml2sp*.
2. Dans la propriété *Le mot de passe de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, entrez le mot de passe de votre magasin de clés SAML 2.0.
   Par défaut, le mot de passe est le même que le nom d'alias par défaut.
3. Cliquez sur **Mettre à jour**.
4. Régénérez vos métadonnées SP.
   Pour plus d'informations, consultez Métadonnées du portail de services.

Créer un magasin de clés de fournisseur de service pour SAML

Créez un magasin de clés Java contenant les éléments suivants pour que votre instance signe les demandes de déconnexion.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

- Certificat de serveur signé pour l'instance
- Certificat CA signé
- Paire de clés publiques et privées

Vous pouvez créer votre propre certificat signé auprès d'une autorité de certification privée ou en acheter un auprès d'une autorité de certification publique.

Les étapes suivantes illustrent comment générer un nouveau fichier de magasin de clés Java Keytool, créer une demande de signature de certificat (CSR) et importer des certificats. Tous les certificats racines ou intermédiaires doivent être importés avant d'importer le certificat primaire pour votre domaine. Tapez ces commandes dans une interface de ligne de commande.

Remarque :
Ces instructions ne sont pas spécifiques à la plateforme et nécessitent des connaissances techniques des certificats de sécurité. L'assistance technique ne peut pas vous aider à créer les certificats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Générez un magasin de clés Java et une paire de clés.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Générez une CSR pour un magasin de clés Java existant.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importez un certificat d'autorité de certification (CA) racine ou intermédiaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importez un certificat primaire signé dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Installation d'un magasin de clés de fournisseur de service pour la signature des demandes SAML

Suivez les étapes suivantes pour supprimer l'exemple de magasin de clés existant et installer votre propre magasin de clés de fournisseur de service contenant votre paire de clés publique et privée.

Avant de commencer

Rôle requis : admin

Procédure

1. Créez un magasin de clés de fournisseur de service.
2. Accédez à la **Authentification unique SAML 2** > **Certificat** ou **Multi-fournisseurs** > **Administrateur** > **Certificat x509**.
3. Cliquez sur **SAML 2.0 Keystore_Key2048_SHA256**.
4. Cliquez sur le lien **Gérer les pièces jointes** .
5. Cochez la case Supprimer en regard de *saml2sp_key2048withsha256.jks*.
6. Cliquez sur **Supprimer**.
7. Cliquez sur **Choisir des fichiers** et sélectionnez le magasin de clés contenant vos certificats signés.
8. Cliquez sur **Joindre**.
9. Fermez la fenêtre contextuelle Pièces jointes.

> **Remarque :**
> Il est recommandé de fournir un nom différent pour le certificat qui vient d'être joint.

10. Dans *Mot de passe du magasin de clés*, saisissez le mot de passe pour accéder à l'alias SAML 2.
11. Cliquez sur **Mettre à jour**.

(Facultatif) Propriétés SAML avancées

Les paramètres avancés suivants vous permettent d'augmenter encore la sécurité et de déboguer l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres avancés

Accédez à la **Tous** > **Authentification unique SAML 2** > **Propriétés**.

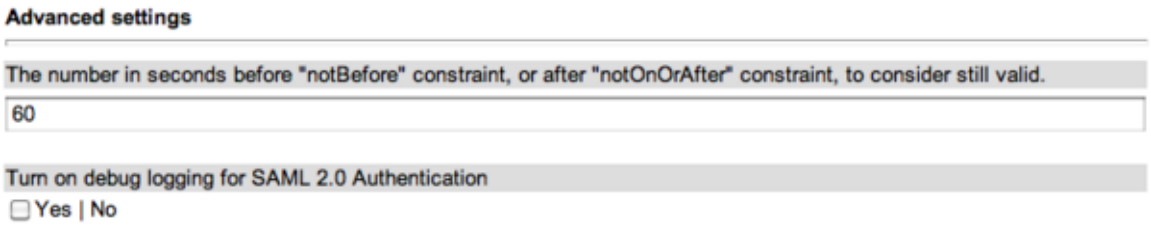


Table des propriétés système avancées

Propriété	Description
Nombre de secondes de contrainte « notBefore », ou après la contrainte « notOnOrAfter », à considérer toujours valables	Saisissez le nombre de secondes à ajouter aux contraintes *NotBefore* et *NotOnOrAfter* pour tenir compte des différences de temps entre l'horloge IdP et l'horloge SP. Ces contraintes empêchent les attaques par rejeu en refusant les demandes qui ne sont pas effectuées dans le délai spécifié. Si l'horloge IdP et l'horloge SP sont très différentes, la latence du réseau peut entraîner le refus de l'autorisation de la demande SAML. Cette propriété ajoute une période de grâce au cours de laquelle les demandes et réponses SAML sont toujours considérées comme valides.
Activez la journalisation du débogage pour l'authentification SAML 2.0	Sélectionnez **Oui** pour activer des informations de journalisation supplémentaires pour les événements SAML 2.0.

Installer le certificat du fournisseur d'identité

Vous pouvez coller un certificat PEM dans un formulaire de certificat X.509 afin que le fournisseur d'identité puisse vérifier les communications avec le fournisseur de service.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le certificat de l'IdP se trouve dans les métadonnées de l'IdP. Le développeur IdP détermine où résident les métadonnées de certificat lors de la création de l'IdP local.

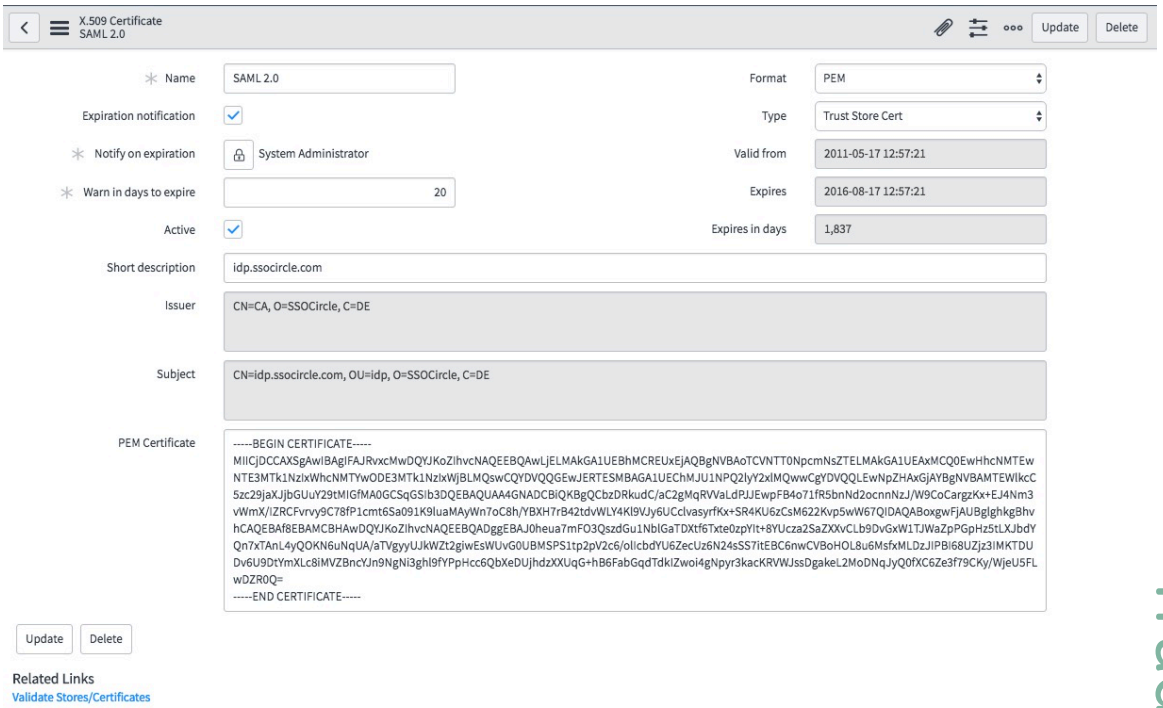
Remarque :
Les certificats pour l'authentification unique doivent toujours être au format PEM pour fonctionner avec les certificats SAML.

Procédure

1. Accédez à la **Tous** > **Authentification unique SAML** > **Certificat**.
2. Renseignez les champs de formulaire (consultez la table).
3. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
L’intégration ne signe pas actuellement le certificat dans les communications entre l’instance et l’IdP.

Champ	Description
Nom	Le nom du certificat. Ne modifiez pas l’entrée *Nom* . Le nom du certificat X.509 doit être *SAML 2.0* pour que l’intégration l’utilise. Cette condition est vraie uniquement si vous n’utilisez pas .Authentification unique (SSO) de plusieurs fournisseurs
Notification d'échéance	Sélectionnez cette option pour envoyer une notification aux utilisateurs sélectionnés dans le champ **Notification à l’expiration** . Cette option est activée par défaut.
Notification à l'expiration	Sélectionnez les utilisateurs pour relancer la notification concernant l’expiration du certificat. Si aucun utilisateur n’est sélectionné, l’utilisateur connecté est ajouté par défaut, ainsi que les deux derniers utilisateurs connectés disposant du rôle d’administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l’expiration à l’origine de l’envoi de la notification par l’instance. Saisissez une valeur d’au moins 20. Cette valeur est définie sur 20 pour les instances mises à niveau vers Istanbul et les versions ultérieures, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher indiquant que ce certificat est actif.
Format	Le format du certificat. SAML utilise le format PEM.
Type	Le conteneur du certificat. L’instance reconnaît les certificats des magasins de clés de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Début de validité	L’instance ajoute automatiquement la date de début de validité du certificat à ce champ. Joignez le certificat à l’enregistrement de certificat X.509 pour remplir ce champ.
Date d'expiration	L’instance ajoute automatiquement la date d’expiration du certificat à ce champ. Joignez le certificat à l’enregistrement de certificat X.509 pour remplir ce champ.
Échéance en jours	Nombre calculé de jours jusqu’à l’expiration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description brève	Description du certificat.
Problème	L'instance ajoute automatiquement l'émetteur du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Objet	L'instance ajoute automatiquement le certificat soumis à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Entrez la valeur du certificat X509.

Que faire ensuite

Cliquez sur **Valider les banques/certificats** pour tester le magasin de confiance et le certificat.

Remplacer un certificat manquant pour SAML

Si le module **Certificat** affiche une page vide, l'enregistrement du certificat SAML 2.0 a été supprimé. Vous pouvez remplacer le certificat manquant en créant manuellement un enregistrement de certificat.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Certificats**.
2. Créez un nouvel enregistrement appelé `SAML 2.0`.

> **Important :**
> Vous DEVEZ utiliser ce nom. Cette condition est vraie uniquement si vous n'utilisez pas .Authentification unique (SSO) de plusieurs fournisseurs

3. Cliquer sur **Authentification unique SAML 2** > **Certificat**.
4. Dans le champ *Certificat PEM* , saisissez la valeur de l'élément `ds :X509Certificate` à partir des métadonnées de votre fournisseur d'identités.
5. Cliquez sur **Enregistrer**.

Tester l'intégration SAML

Testez l'intégration SAML une fois que toutes les autres tâches de configuration sont terminées.

Avant de commencer

Rôle requis : admin

Procédure

1. Connectez-vous à l'instance en tant qu'utilisateur avec le rôle d'administrateur.
2. Accédez à la **Authentification unique SAML 2** > **Propriétés**.
3. Dans la propriété *Activer l'authentification externe*, sélectionnez **Oui**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

L'activation de l'authentification externe nécessite que tous les utilisateurs utilisent l'authentification unique SAML 2.0. Si quelqu'un tente d'accéder à l'application dans un état non authentifié, l'instance envoie automatiquement une demande d'authentification à l'IdP et redirige l'utilisateur vers la page Authentification IdP SAML.

4. Cliquez sur **Enregistrer**.
5. Déconnectez-vous de l'instance.
6. Accédez à l'URL de l'instance.
   Si l'intégration fonctionne correctement, l'IdP doit demander les informations d'identification de l'utilisateur.

Information associée

Erreurs et correctifs Multi-SSO (SAML 2.0)

Erreurs et correctifs Multi-SSO (SAML 2.0)

Une liste des erreurs courantes et des correctifs associés pour une installation et une configuration Multi-SSO (SAML 2.0).

Erreurs lors de la configuration de l'authentification unique (SAML 2.0)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
NotAfter : <Thu Jun 05 22:57:44 PDT 2014>.	Vérifiez que le certificat IDP x509 est présent, valide et actif.	N/A	Le certificat actuel ou l'assertion SAML a expiré.	• Synchronisez l'horloge SNC avec l'horloge du serveur IdP SAML. • Mettez à jour l'enregistrement du certificat SAML 2.0.
• Impossible de localiser le certificat SAML 2.0. • Impossible de trouver une signature numérique stockée dans l'instance ServiceNow.	Vérifiez que le certificat IDP x509 est présent, valide et actif	La chaîne au format PEM doit être saisie dans le champ Certificat PEM.	Le certificat SAML n'existe pas. Il est peut-être inactif.	Assurez-vous que le certificat au format PEM correct est téléchargé sur l'instance.
Les certificats ne correspondent pas. Expect : <certStr>, réel : <inboundCert>.	Vérifiez que le certificat IDP x509	N/A	Le certificat disponible dans SNC ne correspond pas au certificat dans	Confirmez que la chaîne au format PEM dans l'enregistrement du certificat SAML 2.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
	est présent, valide et actif.		l'assertion. Les causes sont les suivantes : • Le certificat est mis à jour sur l'IdP, mais pas sur l'instance ServiceNow. • Le certificat est au mauvais format.	correspond au certificat X509 dans la réponse SAML pour l'IdP de l'utilisateur.
Échec de la vérification de la validité du certificat.	Vérifiez que le certificat IDP x509 est présent, valide et actif	N/A	Le certificat actuel a peut-être expiré.	Mettez à jour l'enregistrement du certificat SAML 2.0.
Échec de la validation du profil de signature.	Vérifiez que le certificat IDP x509 est présent, valide et actif.	N/A	L'assertion peut être signée avec un certificat différent.	Vérifiez si l'IdP dispose du même certificat que l'instance SNC.
InResponseTo dans Incohérence SubjectConfirmationData. Expect : <inResponseTo>, réel : <inResponseTo>.	Échec de la validation de la confirmation d'objet.	N/A	Cette erreur se produit si l'une des situations suivantes se produit : • L'IdP renvoie une SAMLResponse pour une autre SAMLRequest • Un utilisateur crée un signet pour l'URL avec SAMLRequest au lieu de l'URL de l'instance uniquement • Si une valeur nulle est attendue, la réponse peut être envoyée à un autre	L'administrateur IdP doit confirmer que la SAMLReponse attendue est renvoyée. Il peut s'agir d'un problème d'équilibreur de charge ou d'infrastructure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
			nœud lorsque l'instance possède plusieurs nœuds.	
Valeur d'index de session introuvable : <message>...	SessionIndex non valide.	N/A	Le SessionIndex est requis dans l'instance SNC. L'IdP le renvoie dans la réponse SAML pour s'authentifier avec succès.	L'administrateur IdP doit confirmer que l'index de session est défini dans SAMLResponse.
Aucune confirmation d'objet valide trouvée.	Échec de la validation de la confirmation d'objet.	N/A	Des conditions peuvent être manquantes en raison d'une erreur sur IdP. Le StatusCode dans la réponse contiendrait Responder au lieu de la Réussite attendue.	Passez en revue la SAMLResponse pour déterminer si les conditions sont incluses dans la SAMLResponse. Les données de confirmation d'objet valides peuvent expiré ou non pour la bonne audience.
Incohérence de l'audience d'assertion. Expect : <propAudience>, réel : <audienceUri>. ou Échec de la validation de AudienceRestriction. Aucune audience correspondante trouvée.	Vérifiez que le champ 'URI de l'audience' est défini correctement	L'URI du public qui accepte le jeton SAML2. (Il s'agit normalement de votre URI d'instance. Par exemple : https://demo.service-now.com.)	L'URI de l'audience configurée par l'instance SNC doit correspondre à la valeur de l'IdP.	Localisez <saml2 :Audience> dans SAMLResponse dans les journaux et vérifiez que la valeur correspond à celle de l'instance.
L'émetteur de l'assertion n'est pas valide. Expect : <valeur sur l'instance>, actual : <valeur retournée par IdP>	L'émetteur de l'assertion n'est pas valide.	L'URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations	L'ID de l'entité IdP (émetteur) ne correspond pas à la valeur définie dans l'instance SNC.	• Vérifiez si l'IdP ou le SP n'est pas configuré correctement. • Vérifiez que la propriété SAML (l'URL du fournisseur d'identité qui émet

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
		de l'utilisateur.		le jeton de sécurité SAML2 avec les informations de l'utilisateur) est correctement définie.
L'objet est valide dans le futur. Maintenant : <maintenant>, NotBefore : <notBefore> ou L'objet a expiré. Maintenant : <maintenant>, NotOnOrAfter : <notOnOrAfter>	Échec de la confirmation de la validation de l'objet.	Nombre de secondes avant la contrainte notBefore, ou après la contrainte notOnOrAfter, à considérer toujours valable.	L'horloge IdP n'est pas synchronisée avec l'horloge SP.	Mettez à jour la propriété SAML glide.authenticate.sso.saml2.clockskew vers une valeur plus élevée. La valeur par défaut est de 180 secondes. Certains cas nécessitent un paramètre de 300 ou plus. Vous devrez peut-être également vérifier l'heure sur votre serveur IdP.
L'assertion est valide dans le futur, maintenant : <now>, notBefore : <notBefore> ou L'assertion a expiré, maintenant : <now>, notOnOrAfter : <notOnOrAfter>	L'assertion n'est pas valide.	Nombre de secondes avant la contrainte notBefore, ou après la contrainte notOnOrAfter, à considérer toujours valable.	L'horloge IdP n'est pas synchronisée avec l'horloge SP	Augmentez la valeur de la propriété SAML. La valeur par défaut est de 60 secondes. Certains cas nécessitent un paramètre de 300 ou plus. Vous devrez peut-être également vérifier l'heure sur votre serveur IdP.

Erreurs courantes de connexion et d'IdP

Erreur ou symptôme	Diagnostic	Corriger
Les demandes de connexion génèrent une boucle infinie entre le système et l'IdP lorsque la haute sécurité est active.	• En règle générale, le point de terminaison de l'URL est une page d'erreur ou une page de déconnexion. • Le logout_redirect.do peut créer cette boucle lorsque vous définissez *glide.security.url.whitelist*	Définissez (ou créez) le glide.authenticate.failed_redirect de propriété système pour rediriger les demandes d'authentification ayant échoué vers cette URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs courantes de connexion et d'IdP (suite)

Erreur ou symptôme	Diagnostic	Corriger
	sans ajouter le nom d'hôte IdP à la valeur de propriété. **Remarque :** Pour en savoir plus sur cette propriété, consultez Appliquer la vérification de la liste d'autorisations d'URL [Mis à jour dans le Centre de sécurité 1.3, 1.5 et 2.0] Paramètres de renforcement de la sécurité de l'instance.	
Le jeton utilisé pour authentifier l'utilisateur ou la demande est signé avec l'algorithme de signature http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 qui n'est pas l'algorithme de signature attendu http://www.w3.org/2000/09/xmldsig#rsa-sha1.	Vérifiez l'onglet Contexte de l'alerte pour plus de détails sur l'événement.	Accédez à l'onglet Avancé de la boîte de dialogue de configuration de l'approbation de la partie de confiance et vérifiez que l'algorithme est défini sur SHA-1 et non sur SHA-256.
Le message d'erreur urn :oasis :names :tc :SAML :2.0 :status :Requester s'affiche dans votre table journal système (syslog).	Lorsque votre fournisseur d'identité (par exemple, ADFS) répond avec l'état oasis :names :tc :SAML :2.0 :status :Requester, cela signifie qu'il a refusé la connexion en raison d'un problème avec la demande qui lui a été envoyée. Malheureusement, la réponse SAML reçue de l'IdP dans la plupart des cas ne fournit pas plus de détails sur l'erreur.	Examinez la demande SAML envoyée à l'IDP et collaborez avec votre administrateur IdP pour mettre à jour les paramètres SAML de votre instance afin d'éviter l'erreur. Vous devrez peut-être contacter votre fournisseur IDP pour comprendre la raison de l'échec de la connexion.

Rediriger les connexions Single Sign-On (SSO)

Lorsque la SSO est activée, vous pouvez rediriger les utilisateurs vers des pages spécifiques ou demander aux utilisateurs de se connecter localement.

Par exemple, si un utilisateur tente d'accéder à https://customerX.service-now.com, un portail d'entreprise interne peut s'afficher à la place de la page de connexion par défaut. Ou, lorsqu'un utilisateur se déconnecte d'une application, le navigateur peut le rediriger vers une page interne spécifique. Vous pouvez définir des propriétés de redirection au sein de l'instance pour vous assurer que les utilisateurs voient une page de connexion SSO plutôt que la page de connexion par défaut.

Remarque :
Les propriétés suivantes ne forcent pas SSO. La page login.do est toujours accessible et les utilisateurs peuvent se connecter au système s'ils ont défini un mot de passe local.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de la redirection

Lorsqu'un utilisateur se déconnecte, ou en cas d'échec de tentative de connexion à l'aide de l'authentification unique, vous pouvez définir l'emplacement suivant de l'utilisateur, par exemple une page de portail principal ou un article de la base de connaissances avec des informations de connexion SSO. Utilisez les propriétés suivantes pour spécifier les URL. Si l'une de ces propriétés n'existe pas dans votre instance, vous pouvez la créer.

glide.authenticate.failed_requirement_redirect

URL vers laquelle rediriger les utilisateurs lorsqu'ils tentent d'accéder à une page privée (par exemple, pour afficher un incident) et ne fournissent pas d'informations d'identification SSO. La propriété est généralement définie sur le portail de connexion d'un client (par exemple, `http://portal.companya.com/`).

glide.authenticate.failed_redirect

URL permettant de rediriger des utilisateurs après un échec de tentative SSO. Vous pouvez rediriger vers un article de la base de connaissances publique qui décrit l'erreur et contient des liens utiles (par exemple, `http://portal.companya.com/error`).

glide.authenticate.external.logout_redirect

URL permettant de rediriger les utilisateurs après la déconnexion, généralement vers le portail qui a activé la connexion avec authentification unique (par exemple, `http://portal.companya.com/logout`).

glide.authentication.external.disable_local_login

Lorsque la valeur est définie sur vrai, les informations d'identification SSO sont requises pour la page de connexion principale. La valeur par défaut est false. Cette propriété doit être utilisée conjointement avec la *`glide.authenticate.failed_requirement_redirect`* propriété.

Le tableau suivant montre la relation entre les valeurs de retour de sortie d'installation, les propriétés et le comportement attendu.

Connexion forcée à l'aide de l'authentification unique uniquement

Valeur de retour	Propriété	Comportement
failed_missing_requirement	*`glide.authenticate.failed_requirement_redirect`*	Lorsque cette valeur est r indique que les informatio SSO requises ne sont pas session. La connexion éch est redirigée vers l'URL s propriété. Il s'agit généra du fournisseur SSO où la contestée et les informatio sont collectées.
failed_authentication	*`glide.authenticate.failed_redirect`*	Lorsque cette valeur est r indique que les informatio SSO fournies ont échoué que l'utilisateur n'existe p l'utilisateur est verrouillé échoue et la session est re l'URL spécifiée par la pro généralement de l'URL d SSO où la connexion est informations d'identificat

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexion forcée à l'aide de l'authentification unique uniquement (suite)

Valeur de retour	Propriété	Comportement
`<user_id>`	N/A	Connexion autorisée pour par <`user_id`>. Cette v au nom de champ défini d `glide.authenticat` SSO (« nom de champ de comparer à l'en-tête entra

Restriction de la connexion locale

Par mesure de sécurité, vous devez faire plus que vous fier aux propriétés de redirection pour interdire la connexion locale. Si un utilisateur ne doit jamais se connecter localement et sera toujours authentifié par votre système d'authentification unique interne, un mot de passe aléatoire doit être attribué à chaque utilisateur importé dans l'instance. Le mot de passe aléatoire est plus facile à définir au moment de l'importation de l'utilisateur. Si les données utilisateur sont importées dans votre système via un jeu d'importation, vous pouvez créer un script de transformation onBefore à l'aide du code suivant.

```
var r  = new Packages. java. util. Random ( ) ;

var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
) ;

var newPass  = str1  + str2 ;

target. user_password = newPass ;

//password now set to a random string like this:
//qvm81zdrn7cwwylpvw94eebk
```

Cloner une instance avec une intégration SAML

Cloner une instance avec une intégration SAML. Avant de cloner une instance qui utilise SAML 2.0, conservez les paramètres liés à l'authentification unique SAML sur l'instance cible, sinon vous risquez de rendre l'instance cible inaccessible.

Avant de commencer
Rôle requis : admin

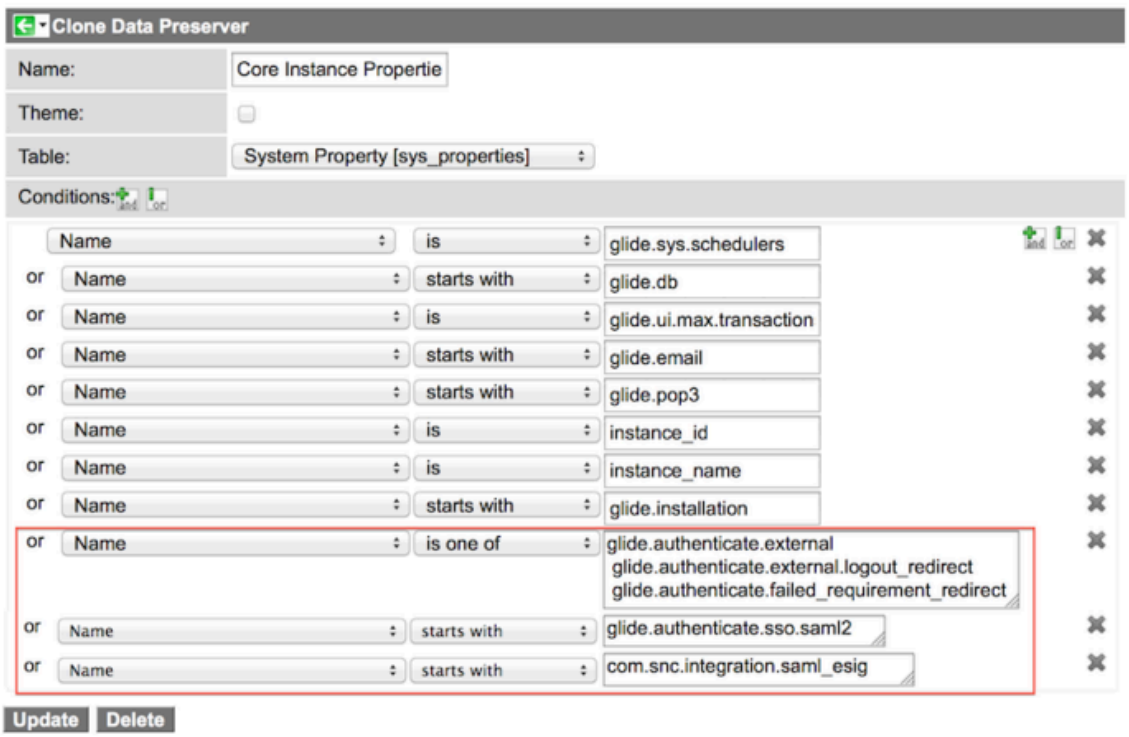
Procédure

1. Sur l'instance source, accédez à **Clone système** > **Conserver les données** > **Propriétés de l'instance principale**.
2. Assurez-vous que les propriétés suivantes liées à SSO SAML sont conservées à l'aide de conditions.
   - glide.authenticate
   - glide.security
   - glide.entrée
   - glide.script
   - glide.session

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig



Remarque :
Lorsque vous créez le clone, incluez des pièces jointes afin que les certificats soient transférés vers l'instance cible. Assurez-vous également que la case **Thème** est décochée afin que ces propriétés soient préservées, que vous conserviez ou non le thème de l'instance.

3. Sur l'instance source, accédez à **Clone système** > **Conserver les données** pour conserver les certificats SAML sur sys_certificate et les utilisateurs SAML sur les sys_user liés à SAML/SSO/Multi SSO.

   Si vous en avez besoin, exportez-les en XML, puis importez-les manuellement sur la cible.

Avertissement :
N'essayez pas de cloner la configuration SAML/SSO/Multi SSO d'un système à un autre. La plupart des transferts des paramètres SAML/SSO ou Multi SSO ne fonctionnent PAS car ils doivent être configurés sur le fournisseur d'identité. Si vous remplacez une configuration de travail, l'instance cible ne parvient pas à s'authentifier et votre instance cible devient inaccessible. De plus, ne modifiez pas le sys_id de votre enregistrement de fournisseur Multi SSO ; Cela obligera vos utilisateurs à purger leurs cookies. Pour plus d'informations sur les précautions de clonage, consultez Liste de vérification avant de cloner une instance .

4. Excluez les tables Multi SSO sso_properties, digest_properties et saml2_update1_properties.
5. Créez manuellement les enregistrements SAML/SSO/Multi SSO sur chaque instance de manière indépendante et configurez également les enregistrements sur votre fournisseur d'identité.
6. Assurez-vous de créer manuellement un compte administrateur LOCAL sur sys_user enregistrement (pas dans LDAP ni SAML) sur l'instance cible et avec un sys_id qui n'existe pas sur l'instance source.
7. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

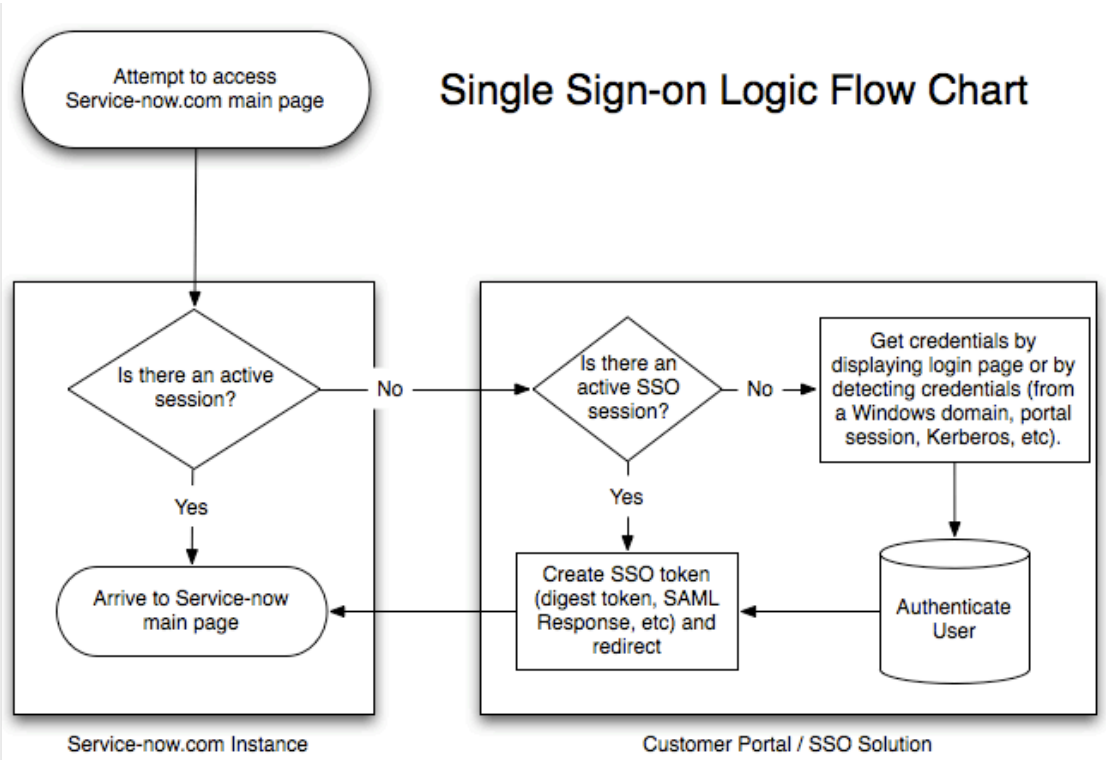
Concepts SAML 2.0

Familiarisez-vous avec ces concepts SAML.

Flux de processus SAML typique (diagramme)

Un flux logique SSO classique implique la recherche d'une session active, la vérification des informations d'identification de l'utilisateur et la création du jeton nécessaire.

SSO Standard



Flux de processus de connexion (AuthnRequest)

SAML 2.0 spécifie un profil SSO de navigateur Web qui implique l'échange d'informations entre un fournisseur d'identité (IdP), un fournisseur de service (SP) et un principal (utilisateur) sur un navigateur Web.

Le fournisseur d'identité peut être n'importe quel service SSO offrant des services d'authentification SAML (par exemple, SSOCircle). Le fournisseur de service est toujours une instance. Le flux de messages commence par une demande de ressource sécurisée auprès du fournisseur de service.

Demander la ressource cible au SP

Le principal demande une ressource cible chez le fournisseur de service :

https://instance.service-now.com/

L'instance vérifie la demande pour voir si les paramètres d'URL SAMLRequest et RelayState sont présents. S'il existe, l'utilisateur a déjà validé avec l'IdP et peut ignorer les étapes 2 à 6.

Émettre une demande AuthnRequest au fournisseur d'identité

L'instance construit une `AuthnRequest` à envoyer à l'IdP à l'aide de la valeur `SAMLRequest` . L'instance construit et envoie également une valeur de paramètre d'URL `RelayState` .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le jeton RelayState est une référence opaque à des informations d'état conservées chez le fournisseur de service. La valeur du paramètre SAMLRequest est la valeur dégonflée et codée en base64 de l'élément <samlp :AuthnRequest> :

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"    ID="identifier_1"
   Version="2.0"    IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy      AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:AuthnRequest>
```

L'intégration code ensuite l'URL de l'élément <samlp :AuthnRequest> et l'envoie en tant que paramètre d'URL SAMLRequest .

Le service SSO traite l'élément <samlp :AuthnRequest> en décodant l'URL, en décodant base64 et en gonflant la demande, dans cet ordre. Il effectue ensuite un contrôle de sécurité. Si l'utilisateur ne dispose pas d'un contexte de sécurité valide, l'IdP l'identifie en l'invitant à saisir ses identifiants de connexion. Si l'utilisateur est déjà connecté, l'IdP répond simplement avec les paramètres d'URL SAMLResponse<tt> et <tt>RelayState (voir étape 3).

Répondre avec SAMLResponse et RelayState

Après avoir collecté les informations d'identification de connexion requises, le service SSO valide la demande et répond avec un document contenant un formulaire XHTML :

```
<formmethod="post"action="https://instance.service-now.com/navpage.do" ...><input
 type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
   ...
   <input type="submit" value="Submit" /></form>
```

La valeur du paramètre RelayState provient de cette étape. La valeur du paramètre SAMLResponse est le codage base64 de l'élément <samlp :Response> suivant :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
 InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
 Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
 IssueInstant="2010-04-29T23:21:51Z"
 Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer><Signature
 xmlns="http://www.w3.org/2000/09/xmldsig#">

...
     </Signature><saml:Subject><saml:NameID
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
         NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameID><saml:Su
bjectConfirmation
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
          InResponseTo="90AA6073F01567BFB0DF194F596314E2"
          NotOnOrAfter="2010-04-29T23:31:51Z"
Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
NotBefore="2010-04-29T23:11:51Z"
NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audience>http
s://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"
SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnContext><sa
ml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Asse
rtion></samlp:Response>
```

Valider la réponse SAML

La valeur SAMLResponse est décodée en base64 et gonflée pour révéler le document XML à l'étape 3. Le script de connexion extrait la valeur XML de l'élément Subject/NameID et l'utilise pour rechercher un utilisateur existant dans la table Utilisateur.

Le script de connexion extrait également l'ID de session de l'élément AuthnStatement/@SessionIndex et le stocke pour LogoutRequest.

Flux de processus de déconnexion (LogoutRequest)

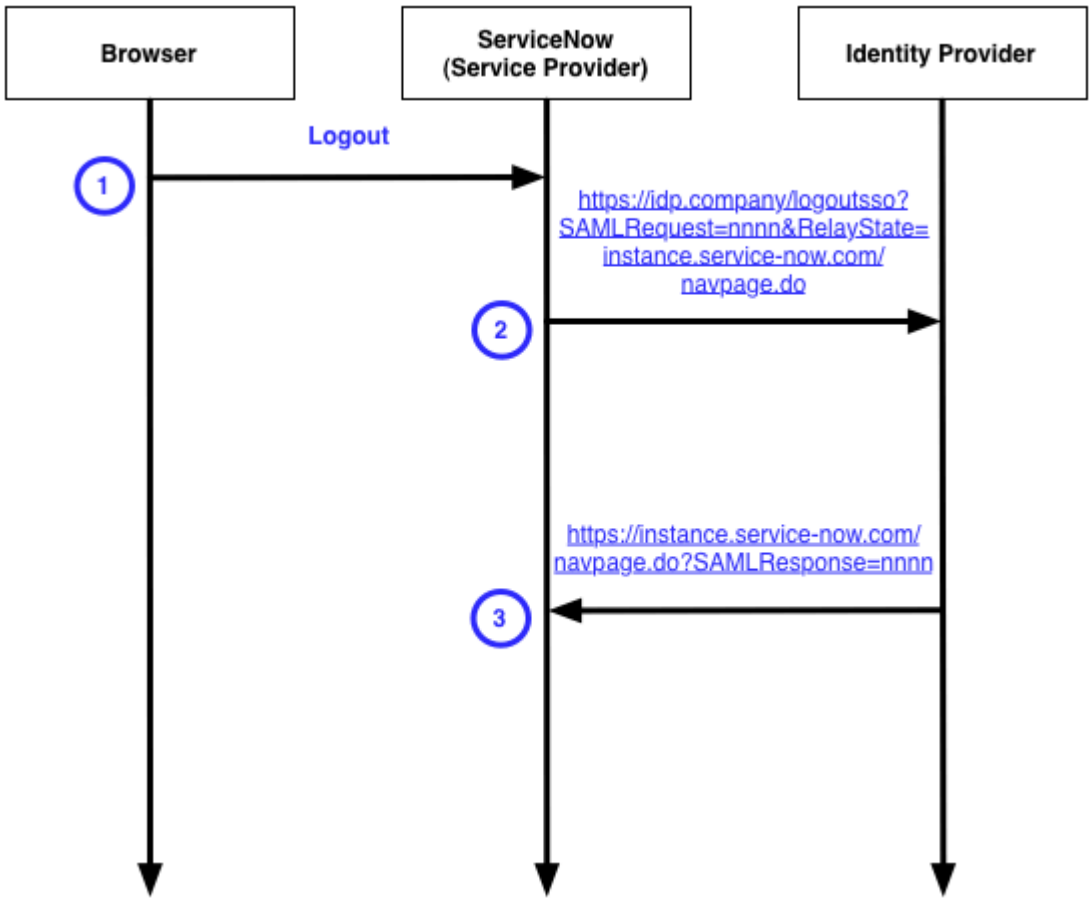
Pendant la déconnexion, l'instance émet l'appel de service *LogoutRequest* SAML 2.0 à l'IdP.

Ce service déconnecte l'utilisateur, puis le redirige vers l'URL de déconnexion spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déconnexion SAML 2



L'utilisateur clique sur le bouton Déconnexion

L'utilisateur clique sur le bouton **Déconnexion** et l'instance exécute le script de déconnexion.

Déconnexion émise

Le script de déconnexion construit une `LogoutRequest` SAML 2.0 et la publie sur le service SAML 2.0 préconfiguré SingleLogoutRequest au niveau de l'IdP. L'IdP dégonfle la demande, puis base64 l'encode. Un exemple de `LogoutRequest` ressemble à ceci :

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"  IssueInstant="2010-04-28T21:36:11.230Z"
 Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://dloomac.service-now.com
 </saml2:Issuer><saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID><saml2
p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

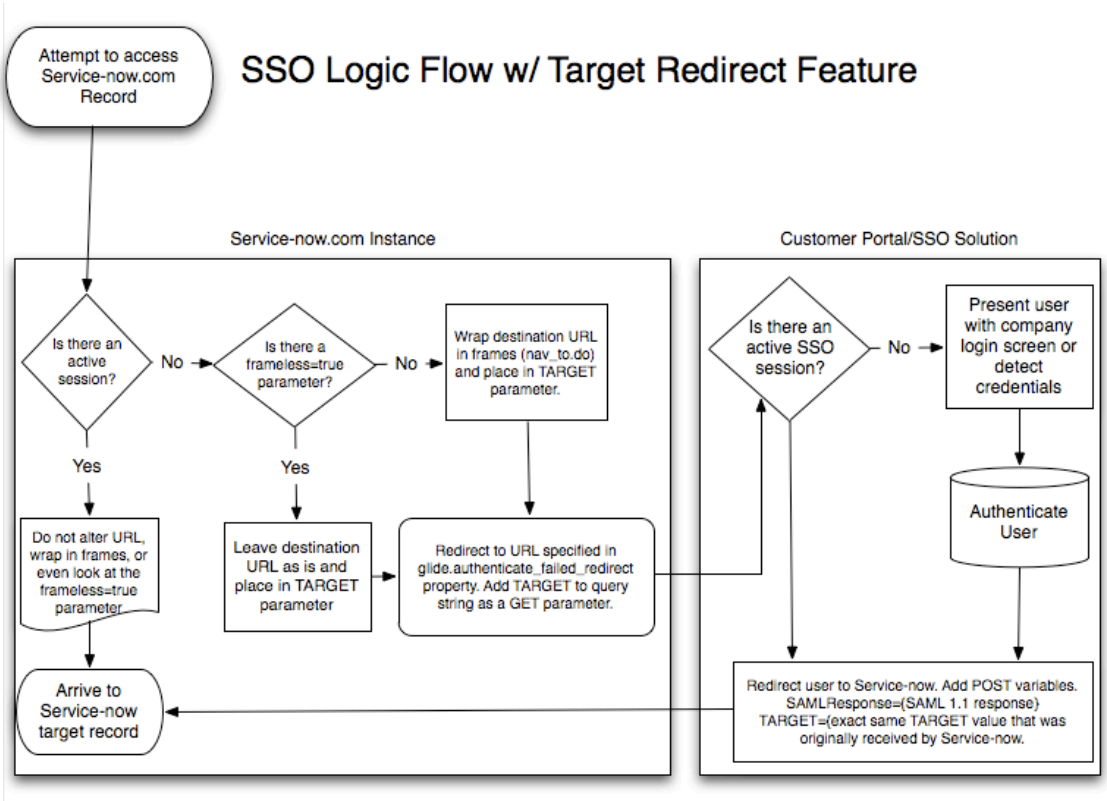
L'utilisateur se déconnecte

L'utilisateur se déconnecte de l'IdP. L'IdP redirige vers l'instance, qui à son tour redirige vers l'IdP puisque l'utilisateur n'est pas connecté.

Informations sur l'URL d'un fournisseur SSO

Lors d'une contestation de connexion résultant d'un lien URL vers l'instance qui nécessite une session SSO, l'URL de référence peut devoir être fournie au fournisseur SSO afin qu'après authentification, l'URL puisse être renvoyée à l'instance et liée à la ressource appropriée.

Redirection de cible SSO



Les valeurs de retour de sortie de l'installation ont été améliorées pour transmettre une URL à la place ou en plus de l'URL définie par les propriétés. En règle générale, vous renvoyez un nom d'utilisateur ou une valeur de chaîne prédéfinie pour contrôler, autoriser ou contester la session SSO. Les exemples suivants montrent le comportement étendu de la transmission d'une URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

L'exemple ci-dessus transmet le https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345 d'URL au fournisseur SSO sous la forme d'un paramètre d'URL nommé TARGET.

Remarque :
Il est supposé que le fournisseur SSO utilisera ces informations dans le paramètre TARGET pour rediriger vers l'instance lorsque les informations d'identification de l'utilisateur ont été collectées et que l'authentification a été réussie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un deux-points : délimite les deux valeurs de retour et un & codé (%26amp ;) concatène l'URL définie dans la propriété *glide.authenticate.failed_missing_requirement* et le paramètre TARGET.

Configuration SAML 2.0 à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs

Vous pouvez créer ou mettre à jour une configuration SSO SAML 2.0 à partir de la fonctionnalité SSO de plusieurs fournisseurs.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :
Nouveauté de la Jakarta version, vous devez valider votre configuration à l'aide de la fonctionnalité Test de la connexion avant de pouvoir activer votre configuration IdP. Vous pouvez toujours utiliser la fonctionnalité de mise à jour pour enregistrer vos données de configuration, mais il ne s'agit pas d'une configuration active sans une connexion de test réussie.

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Effectuez l'une des actions suivantes.
   - Pour mettre à jour une configuration, cliquez sur un enregistrement de configuration SSO.
   - Pour créer une configuration, cliquez sur **Nouveau** > **SAML**.
3. Saisissez les informations IdP en utilisant l'une des méthodes suivantes.

Option	Description
Utilisation d'une URL de descripteur de métadonnées	Cliquez sur la case à cocher URL et entrez l'URL de l'IdP que vous utilisez.
Utilisation du fichier XML du descripteur de métadonnées	Cochez la case XML et collez les données XML générées à partir de l'IdP que vous utilisez.
Saisie manuelle des métadonnées	Fermez la fenêtre contextuelle et saisissez manuellement les données dans les champs de propriété.

Remarque :
Tous les champs obligatoires doivent être renseignés dans le formulaire Fournisseur d'identité.

Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	Saisissez le nom de l'IdP. Cet IdP est l'ID système de redirection automatique.
Actif	Oui	Actif doit être défini sur vrai pour que l'IdP soit utilisé pour l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Obligatoire	Description
		Remarque : L'option permettant de définir cette propriété n'intervient qu'après un test de la connexion réussi.
Par défaut	Non	L'IdP de redirection automatique, anciennement appelé fournisseur d'identités principal, redirige automatiquement les utilisateurs vers l'URL de l'instance de base. Cette propriété définit cette configuration IdP par défaut.
Rediriger automatiquement l'IdP	Non	Définit cette configuration IdP en tant qu'IdP de redirection automatique. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est mis à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système, automatiquement activée, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	Saisissez l'URL de votre fournisseur d'identités. Chaque URL IdP doit être unique.
Service AuthnRequest du fournisseur d'identité	Oui	Entrez l'URL de la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService.
Service SingleLogoutRequest du fournisseur d'ident	Non	Entrez l'URL obtenue à partir de l'élément SingleLogoutService.
ServiceNow Page d'accueil	Oui	Entrez l'URL, y compris la page de connexion, de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/navpage.do
ID d'entité/émetteur	Oui	Entrez l'URL de base, à l'exclusion de la page de connexion. de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
URI de l'audience	Oui	Entrez l'URL de base, à l'exclusion de la page de connexion. de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
Politique NameID	Oui	Entrez la valeur de l'élément NameIDFormat que l'intégration utilise.
Redirection de déconnexion externe	Non	Entrez l'URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion.
Échec de la redirection du besoin	Non	Entrez l'URL de redirection des demandes d'authentification ayant échoué. Par défaut, il s'agit du point de terminaison d'URL d'une page d'erreur ou d'une page de déconnexion configurée dans l'IdP. Vous pouvez renseigner cette valeur dans le champ glide.authenticate.failed_requirement_redirect.
Type de client	Non	Choisissez le type de client, en fonction du type de votre client. Options :**Iframe incorporé**.

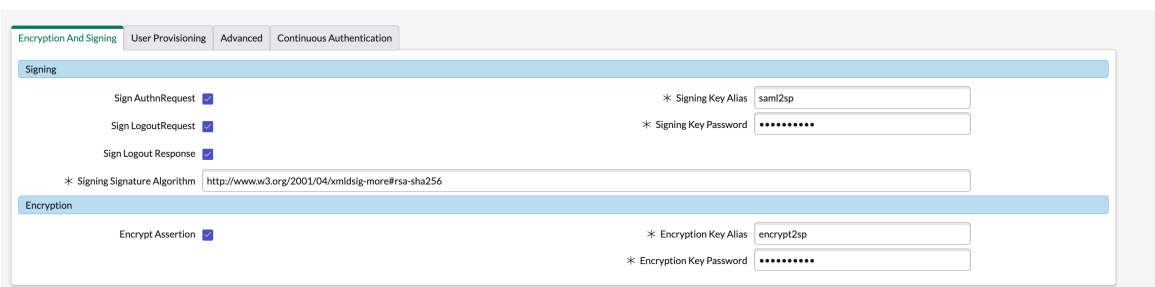
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Obligatoire	Description
		Remarque : Si le champ Type de client est requis pour votre configuration, vous pouvez modifier le formulaire et ajouter le champ. Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

4. **Facultatif :** Onglet Chiffrement et signature

Remarque :

- Il est recommandé d'utiliser vos propres certificats pour le chiffrement et la signature.
- Le **mode approuvé par FIPS** nécessite différents certificats pour **le chiffrement et lasignature**
- Lors de l'utilisation des certificats, assurez-vous de mettre à jour les propriétés système suivantes avec la sys_id des certificats (certificats x.509) :
  - **Signature** (glide.authenticate.sso.saml2.keystore)
  - **Chiffrement** (glide.authenticate.sso.saml2.encryption.keystore)
- Assurez-vous de mettre à jour l'alias de clé et le mot de passe de clé des magasins de **clés de signature** et **de chiffrement** dans l'enregistrement du fournisseur d'identité et de générer les métadonnées (sélectionnez **Générer les métadonnées**).
- Chargez les certificats de signature et de chiffrement présents dans les métadonnées générées (XML) vers le fournisseur d'identité.



Champs de chiffrement et de signature

Propriété	Description
Signature avec l'alias de clé	Entrez l'alias de signature de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Signature avec le mot de passe de clé	Entrez le mot de passe de signature de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Alias de clé de chiffrement	Entrez l'alias de chiffrement de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Mot de passe de clé de chiffrement	Entrez le mot de passe de chiffrement de la saisie de clé stockée dans le magasin de clés SAML 2.0 SP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

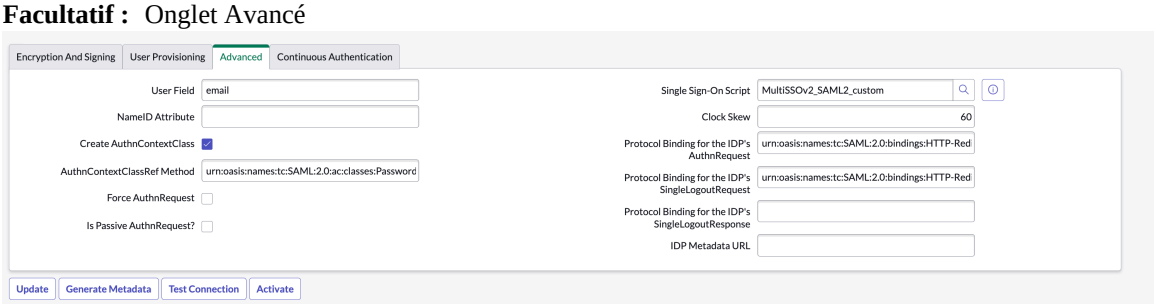
Propriété	Description
Chiffrer l'assertion	Cochez la case pour chiffrer l’assertion dans la réponse SAML. Les métadonnées générées pour l’IDP incorporent le certificat x509, que l’IDP utilise pour chiffrer l’assertion dans la réponse SAML qu’il génère.
Algorithme de signature pour la signature	Entrez l’URL qui pointe sur le consommateur AuthnRequest du fournisseur d’identité SAML 2.0 pour l’authentification de signature électronique.
Signer l'AuthnRequest	Cochez la case pour activer le service d’authentification unique IdP pour recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Cochez cette case pour activer le service d’authentification unique IdP pour recevoir une LogoutRequest.
Signer la réponse de déconnexion	Cochez cette case pour activer le service d’authentification unique IdP afin de recevoir une réponse de déconnexion signée.

5. **Facultatif :** Onglet Attribution d’utilisateurs

Champs d’attribution d’utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	Activer la mise en service automatique d’un utilisateur, crée les utilisateurs lorsque l’utilisateur n’existe pas dans l’instance Table des utilisateurs sur la base des informations fournies par l’IdP.
Mettre à jour l'enregistrement utilisateur à chaque connexion	Met à jour les informations utilisateur dans la table Utilisateur de l’instance avec les informations dans l’IdP chaque fois que l’utilisateur se connecte à l’aide de SAML.

6. **Facultatif :** Onglet Avancé



Champs avancés

Propriété	Description
Champ d'utilisateur	Saisissez le champ de la table Utilisateur qui contient la valeur requise par l’IdP pour identifier l’utilisateur. Il s’agit d’un ID unique dans le cadre de la réponse. Par exemple, nom d’utilisateur, ID d’employé, etc. Dans la table utilisateur système, cet ID unique est mis en correspondance avec les détails de l’utilisateur.
Attribut NameID	Laissez ce champ vide, sauf si vous configurez une nouvelle politique NameID. Si vous configurez une nouvelle politique, le système nécessite la table Utilisateur qu’il doit utiliser pour identifier l’utilisateur qui se connecte. Le système associe le jeton NameID au nom de ce champ de table Utilisateur ici.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Créer une AuthnContextClass	Cochez la case pour spécifier une classe de contexte particulière, telle que Transport protégé par mot de passe. Si la case n'est pas cochée, l'IdP sélectionne la classe de contexte la plus appropriée.
Méthode AuthnContextClassRef	Entrez l'URN du mécanisme de connexion que vous souhaitez que l'IdP utilise pour authentifier les utilisateurs.
Forcer l'AuthnRequest	Cochez cette case pour forcer l'exécution des AuthnRequest.
Est une AuthnRequest passive	Cochez la case si l'AuthnRequest est passive.
Script d'authentification unique	Sélectionnez le script Authentification unique. La valeur par défaut est *MultiSSOV2_SAML2_custom*.
Signer la réponse de déconnexion	Saisissez les détails de la réponse de déconnexion dans ce champ.
Décalage d'horloge	Entrez le nombre de secondes entre les deux attributs qui composent le nonce de la réponse SAML. La valeur par défaut est 60. Une SAMLResponse valide doit se situer entre les valeurs *date-heure notBefore* et *notOnOrAfter* . Voir Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour un exemple de message SAMLResponse.
Protocole de liaison du service SingleLogoutReuqest de l'IDP	Entrez l'une des valeurs prises en charge répertoriées dans l'attribut Binding à partir de l'élément SingleLogoutService.
URL des métadonnées à partir de laquelle les propriétés IDP sont importées	Les propriétés IdP sont importées à partir de cette URL. Si activé, il active l'importation automatique du certificat SAML à partir de l'IdP si le certificat précédent a expiré. **Remarque :** Si vous effectuez une mise à niveau de SAML2 Update 1 vers l'authentification unique (SSO) de plusieurs fournisseurs ou si vous configurez manuellement votre connexion SSO, l'URL des métadonnées IdP n'est pas automatiquement renseignée.
Demande	Un ID unique dans le cadre de la demande. Il peut s'agir d'un nom d'utilisateur, d'un ID d'employé, etc. **Remarque :** La redirection et la liaison de publication sont toutes deux prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après un test de la connexion réussi. Pour plus d'informations, reportez-vous à la section Tester les connexions IdP.
Réponse	Un ID unique dans le cadre de la réponse, l'ID peut être un nom d'utilisateur, un ID d'employé...

Traduction automatique

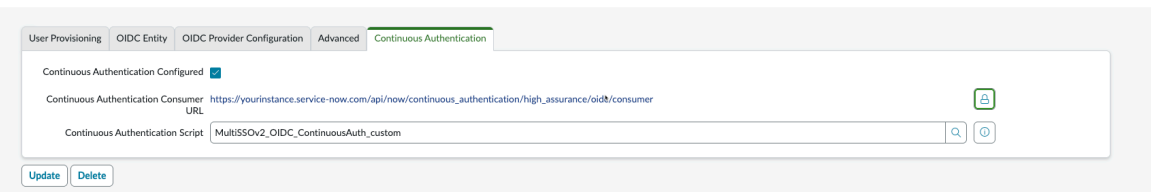
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : La redirection et la liaison de publication sont toutes deux prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après un test de la connexion réussi. Pour plus d'informations, reportez-vous à la section Tester les connexions IdP.

7. **Facultatif :** Dans l'onglet Authentification continue, configurez les champs suivants :

Remarque :

- L'onglet Authentification continue s'affiche uniquement lorsque vous installez le module d'extension **Authentification Zero Trust - continue** (com.snc.zero_trust_continuous_authentication) qui nécessite une licence.
- Si vous utilisez la stratégie d'authentification continue pour protéger l'accès à la table ou à la classe de données, reportez-vous à la section Authentification continue (CA).



Authentification continue

Champ	Description
Authentification continue configurée	Cochez la case pour activer la configuration.
URL du consommateur de l'authentification continue	Fournissez l'URL du consommateur à partir du fournisseur d'identité.
Script d'authentification continue	(Optional) Sélectionnez l'icône de recherche pour choisir le script fourni dans la plateforme. Dans cette configuration, pour SAML : **MultiSSOv2_SAML2_ContinuousAuth_custom**

Certificats X.509 pour SAML

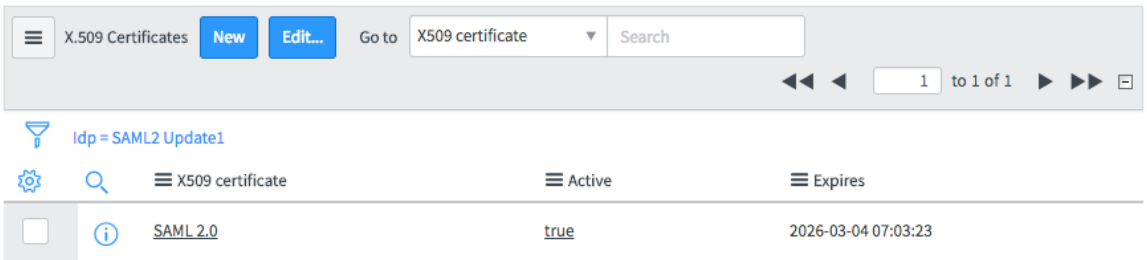
Stockez et activez les certificats d'IdP nécessaires pour votre configuration SAML.

Les certificats X.509 sont les certificats IdP qu'une configuration SAML utilise. Après avoir installé un certificat, vous pouvez ajouter autant de certificats que nécessaire. Lorsqu'il existe plusieurs certificats, le système utilise le premier certificat actif trouvé. Si vous définissez l'URL pour le **champ URL de métadonnées à partir de laquelle les propriétés IDP sont importées**, le système interroge automatiquement l'IdP à la recherche d'un certificat valide lorsque votre certificat n'est plus valide. Il ajoute ce certificat à votre instance et l'utilise pour votre configuration SAML active.

Remarque :
L'interrogation a lieu si l'IdP est accessible en dehors de votre réseau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Visite guidée SAML

Utilisez la visite guidée SAML pour configurer SAML pour l'authentification unique.

La visite guidée SAML vous aide à vous former et à configurer l'authentification unique pour votre ServiceNow® instance. Les administrateurs peuvent sélectionner la visite guidée pour connaître rapidement les actions requises lors de la configuration de SSO pour les instances.

Avant d'utiliser la visite guidée, vous devez configurer une application SAML dans votre fournisseur d'identité préféré, tel que Okta, Microsoft Azure ADFS, etc. Pour savoir comment configurer une application SAML, consultez la documentation suivante :

- Okta: pour Okta, vous devez effectuer les opérations suivantes :
  - Ajouter une application SAML Okta
  - Configurer SAML 2.0 pour ServiceNow®
- Microsoft Azure: Intégration de l'authentification unique (SSO) avec ServiceNow®
- Ping: Configuration de l'authentification unique SAML avec ServiceNow®
- ADFS : Intégration à SAML 2.0

Pour utiliser la visite guidée SAML, activez le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs. Pour plus d'informations, reportez-vous à la section Activer le module d'extension SSO de plusieurs fournisseurs.

Pour utiliser la visite guidée SAML, procédez comme suit :

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseur d'identité**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **SAML**.
4. Cliquez sur l'icône **Aide** .
5. Cliquez sur **Suivre une visite guidée**.

La visite guidée SAML utilise une série d'étapes qui s'étendent sur plusieurs pages pour terminer la configuration, en suivant les étapes et les instructions fournies dans le cadre de la visite guidée et terminer la visite. Pour en savoir plus sur la configuration SAML, reportez-vous à la section Configuration SAML 2.0 à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrer SAML 2.0 à d'autres fonctionnalités

Vous pouvez intégrer votre solution SAML 2.0 à d'autres fonctionnalités telles que la signature électronique, le lien profond et ADFS.

Ajouter la prise en charge du lien profond pour SAML

Le lien profond permet aux instances de prendre en charge les liens directs vers un enregistrement particulier du système.

Lorsque l'intégration SAML 2.0 est activée, les URL de lien profond doivent passer une vérification d'authentification avant que l'IdP ne redirige l'utilisateur vers l'URL initialement demandée. Par exemple, considérez un e-mail qui contient cette URL : `https://<nom d'instance>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`

L'instance envoie une demande d'authentification à l'IdP et utilise le paramètre `URL RelayState` pour préserver la ressource demandée à l'origine (dans ce cas, `uri=incident.do ?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`). Une fois que l'IdP a authentifié l'utilisateur, l'instance lit la valeur du paramètre URL RelayState et redirige l'utilisateur vers la ressource demandée (si elle existe dans l'instance).

Pour ajouter la prise en charge du lien profond, vérifiez que le fournisseur d'identité prend en charge le paramètre `URL RelayState` .

Intégration d'ADFS à SAML 2.0

Le ServiceNow module d'extension SSO de plusieurs fournisseurs prend en charge une intégration SAML 2. Single Sign-On (SSO) avec Microsoft ADFS.

Pour plus d'informations sur l'installation et la configuration d'ADFS, voir Vue d'ensemble des services de fédération Active Directory . Le module d'extension SSO de plusieurs fournisseurs a été configuré et testé avec une intégration SSO SAML 2.0 avec ADFS 2.0, 3.0, Azure AD.ributes ne prennent pas en charge la réponse SAML dans

Configurer ADFS pour SAML

Configurez ADFS pour SAML. Cette procédure utilise ADFS 2.0 et affiche samportal.example.com comme site Web ADFS. Remplacez-la par l'adresse de votre site Web ADFS.

Avant de commencer

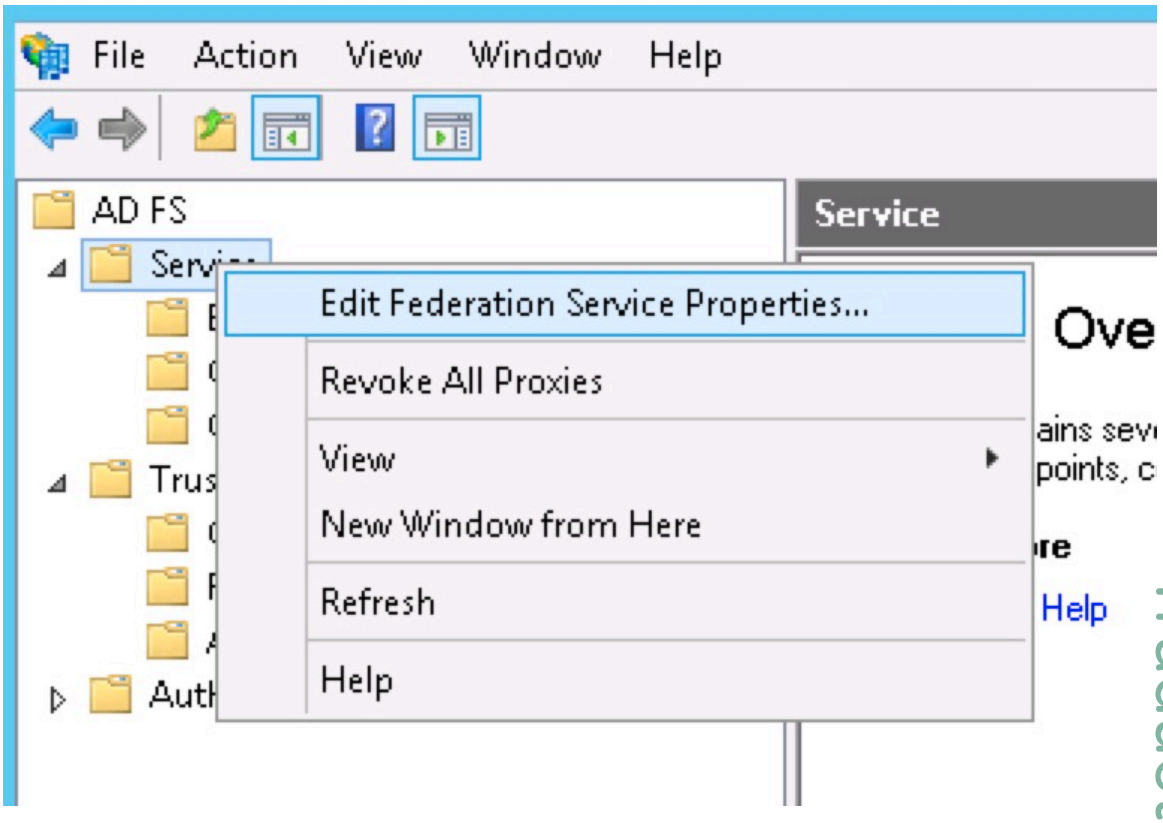
Rôle requis : admin

Procédure

1. Connectez-vous au serveur ADFS 3.0 et ouvrez la console de gestion.
2. Cliquez avec le bouton droit sur **Service** et sélectionnez **Modifier les propriétés du service de fédération**.

Traduction automatique

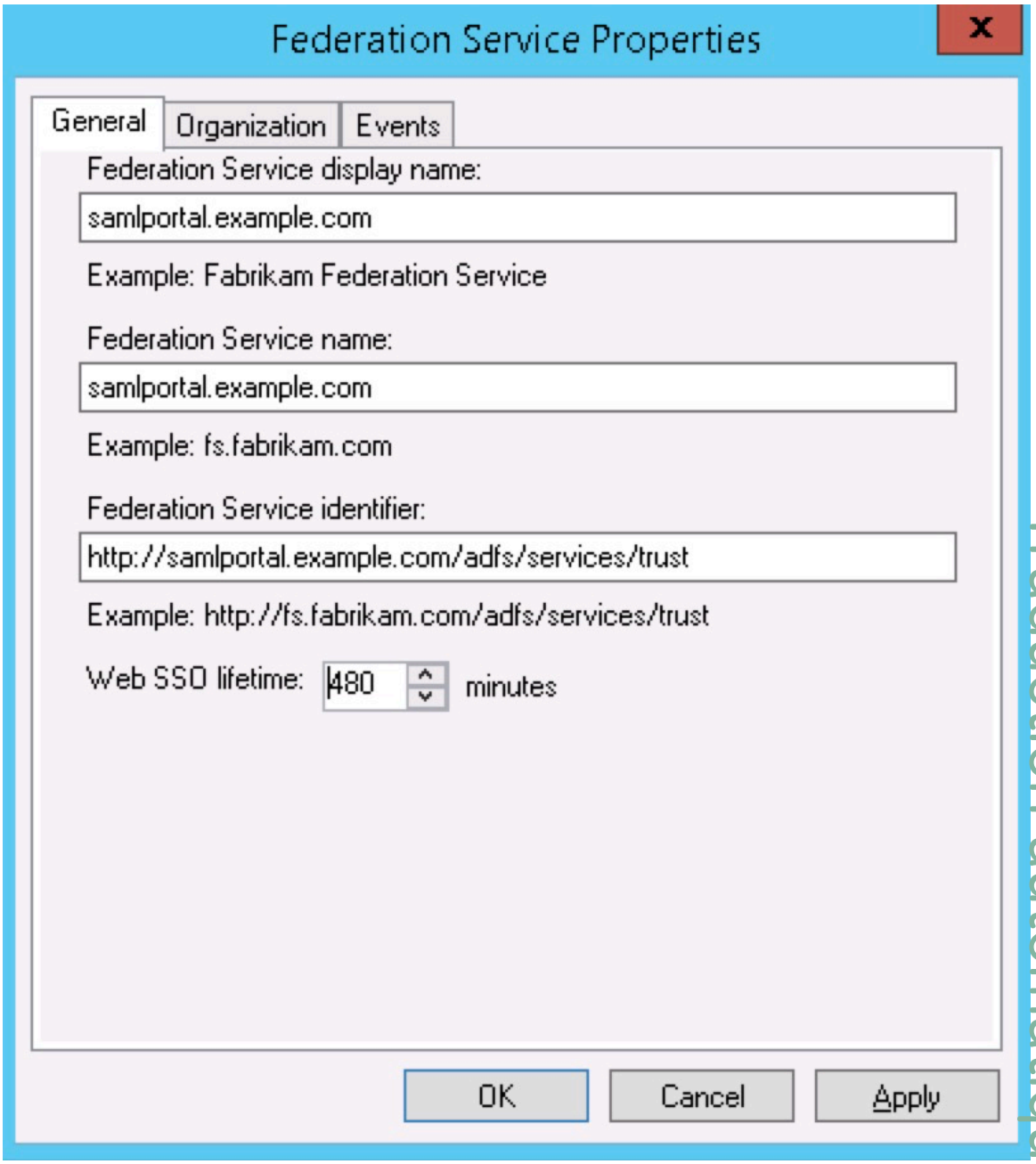
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Vérifiez que les paramètres généraux correspondent à vos entrées DNS et noms de certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Accédez aux certificats et exportez le certificat de signature de jeton.

   a. Cliquez avec le bouton droit sur le certificat et sélectionnez **Afficher le certificat**.

   b. Sélectionnez l'onglet **Détails**.

   c. Cliquez sur **Copier dans le fichier**.
   L'assistant d'exportation du certificat s'ouvre.

   d. Sélectionnez **Suivant**.

   e. Assurez-vous que l'option **Non, ne pas exporter la clé privée** est sélectionnée, puis cliquez sur **Suivant**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Sélectionnez **le binaire codé DER X.509 (.cer),** puis cliquez sur **Suivant**.

g. Sélectionnez l'endroit où vous souhaitez enregistrer le fichier et donnez-lui un nom, puis cliquez sur **Suivant**.

h. Sélectionnez **Finish** (Terminer).
L'instance nécessite que ce certificat soit au format PEM. Vous pouvez convertir ce certificat à l'aide d'outils clients ou d'outils en ligne tels que SSL Shopper.

5. Utilisez le certificat DER/Binary que vous venez de créer et exportez-le au format PEM standard.

Configurer l'instance pour ADFS

Configurez votre instance et les paramètres SAML 2.0 pour qu'ils fonctionnent avec ADFS.

Avant de commencer
N'effectuez ces étapes qu'après avoir configuré ADFS pour SAML. Pour plus d'informations sur ce processus, voir Configuration d'ADFS pour SAML.

Rôle requis : admin

Procédure

1. S'il n'est pas déjà actif, Activer le module d'extension SSO de plusieurs fournisseurs.
2. Configurez SAML, mais lorsque vous installez le certificat IdP, joignez le certificat PEM que vous avez créé lorsque vous Configurer ADFS pour SAML.
3. Cliquez sur **Enregistrer**.
4. Vérifiez que les champs **Problème** et **Objet** contiennent des valeurs et qu'il n'y a pas d'erreurs.
Si une erreur se produit, ouvrez le certificat au format PEM enregistré dans le Bloc-notes et copiez et collez le certificat dans le champ Certificat PEM.
5. Vérifiez que la sortie de l'installation SAML2SingleSignon_update1 est active.
6. Poursuivez la configuration SAML 2.0.

Remarque :
Lorsqu'un certificat est mis à jour sur le serveur ADFS, vous devez également charger un certificat mis à jour dans l'instance.

Configurer une partie de confiance ADFS

Prenez les métadonnées de l'instance et importez-les dans votre serveur ADFS. Toutefois, la configuration manuelle de la partie de confiance semble plus facile à mettre en œuvre.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** > **Mise à jour SAML2 1** > **Chiffrement et signature** et vérifiez que la propriété SAML Signer l'AuthnRequest (`glide.authenticate.sso.saml2.require_signed_authnrequest`) n'est pas active.
Ne conservez cette propriété active que si votre administrateur ADFS peut vérifier que vous avez besoin de demandes signées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Copiez les métadonnées que vous avez générées via le lien de métadonnées SAML 2 et enregistrez-les dans un fichier.
3. Connectez-vous au serveur ADFS et ouvrez la console de gestion.
4. Sélectionnez **les fiducies de partie de confiance**.
5. Sélectionnez **Ajouter une fiducie de partie de confiance** dans le coin supérieur droit de la fenêtre.

   L'assistant d'ajout apparaît.
6. Cliquez sur **Démarrer** pour commencer.
7. Utilisez l'option **Importer un fichier** pour importer le fichier de métadonnées.
8. Donnez-lui un nom d'affichage tel que ServiceNow et entrez les notes de votre choix.
9. Sélectionnez **le profil ADFS 3.0**.
10. Ne sélectionnez pas de certificat de chiffrement de jeton.
    Il utilisera le certificat qui est défini sur le service qui a déjà été exporté. La définition d'un certificat empêche une communication correcte avec l'instance.
11. N'activez aucun paramètre sur **l'URL de configuration**.
12. Entrez le site de l'instance auquel vous vous êtes connecté en tant qu'identificateur de confiance de partie de confiance.
    Dans ce cas, utilisez https://company.service-now.com et cliquez sur **Ajouter**.
13. Autorisez tous les utilisateurs à accéder à cette partie de confiance.
14. Cliquez sur **Suivant** et désactivez la case **à cocher Ouvrir les réclamations à la fin** .
15. Fermez cette page.
    La nouvelle fiducie de partie de confiance apparaît dans la fenêtre.
16. Cliquez avec le bouton droit sur l'approbation de la partie de confiance et sélectionnez **Propriétés**.
17. Accédez à l'onglet **Avancé** et définissez **l'algorithme de hachage sécurisé** sur SHA-256 ou SHA-1.
18. Accédez à l'onglet Points de terminaison et ajoutez un **consommateur d'assertion SAML** avec une liaison **Post** et une URL de https://company.service-now.com/navpage.do.

Configurer les règles de réclamation de la partie de confiance ADFS

Modifiez les règles de réclamation pour permettre une communication appropriée avec l'instance.

Avant de commencer

Rôle requis : admin

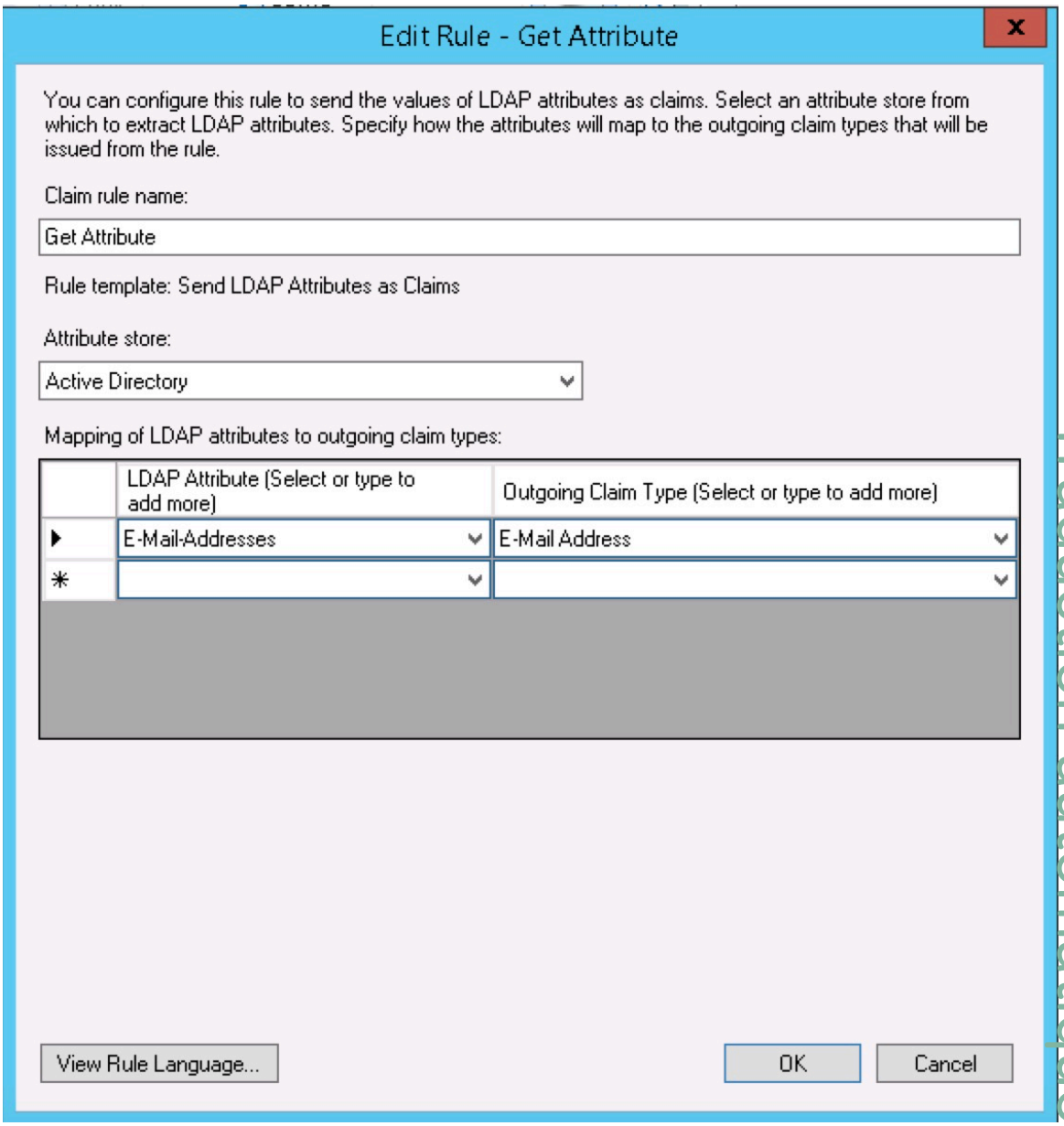
Procédure

1. Connectez-vous au serveur ADFS et ouvrez la console de gestion.
2. Cliquez avec le bouton droit sur l'approbation de la partie de confiance et sélectionnez **Modifier les règles de réclamation**.
3. Cliquez sur l'onglet **Règles de transformation d'émission** .
4. Sélectionnez **Ajouter des règles**.
5. Sélectionnez **Envoyer l'attribut LDAP en tant que réclamations comme modèle** de règle de réclamation à utiliser.
6. Donnez à la réclamation un nom tel que Obtenir des attributs LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Définissez le **magasin d'attributs** sur Active Directory, l'attribut **LDAP** sur Adresses e-mail et le **type de réclamation sortante** sur Adresse e-mail.




```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. Sélectionnez **Finish** (Terminer).
9. Sélectionnez **Ajouter des règles**.
10. Sélectionnez **Transformer une déclaration entrante** comme modèle de règle de déclaration à utiliser.
11. Donnez à la réclamation un nom tel que E-mail à l'ID de nom.
12. Définissez le **type de réclamation entrante** sur le **type de réclamation sortante** dans la règle précédente.

Traduction automatique

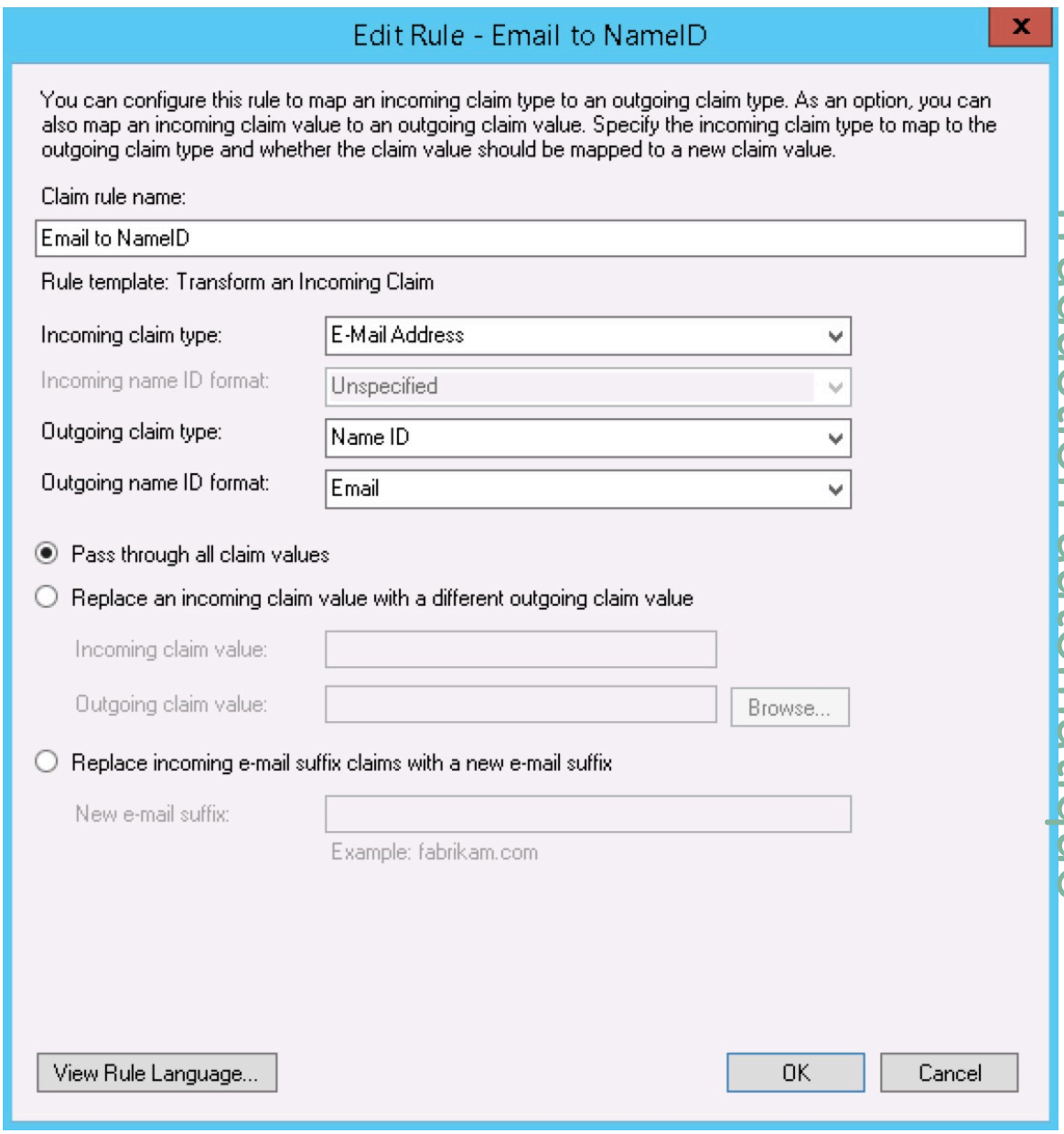
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, l'adresse e-mail.

13. Définissez le **type de réclamation sortante** sur ID de nom et le **format d'ID de nom sortant** sur E-mail.

> **Remarque :**
> Ces valeurs doivent correspondre à la politique d'ID de nom que vous avez définie lors de la configuration SAML 2.0.

14. Sélectionnez **Transmettre toutes les valeurs de réclamation**.



Cette règle de réclamation doit ressembler au langage de règle suivant.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Cliquez sur **Terminer**.

Créer un point de terminaison de déconnexion SAML

Créez un point de terminaison de déconnexion SAML pour autoriser une déconnexion unique.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Pour plus d'informations , consultez cet article sur la déconnexion d'ADFS .

Procédure

1. Accéder à **Gestionnaire ADFS** > **Relations de confiance** > **Approbations de parties de confiance** > **Propriétés de**.
2. Sous l'onglet Endpoints, cliquez sur **Ajouter SAML.**
3. Configurez les paramètres :
   - **Type de point de terminaison** : déconnexion SAML
   - **Liaison** : POST
   - **URL approuvée : URL** de votre serveur ADFS. Par exemple :

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **URL de réponse : URL** de déconnexion de l'application. Par exemple :

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Tester la configuration ADFS

Testez votre configuration ADFS pour vérifier qu'elle fonctionne correctement en tant que fournisseur d'identité.

Avant de commencer
Rôle requis : admin

Procédure

1. Ouvrez un navigateur Internet Explorer.
2. Accédez à votre portail ADFS.

   Par exemple, `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx`. Cette page contient une liste déroulante de toutes les approbations de partie de confiance configurées.

3. Sélectionnez la partie de confiance associée à votre instance.
4. Cliquez sur **Continuer pour vous connecter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous avez correctement configuré l'authentification externe SAML 2.0, vous devriez être automatiquement connecté à l'instance.

5. Testez une URL de connexion directe en accédant à https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com.

(Solution de contournement) Activer l'authentification initiée par le fournisseur de service

Utilisez cette solution de contournement si l'authentification échoue parce que vous ne disposez pas de SAML 2.0 Update 1. Ce problème peut se produire si les utilisateurs tentent d'ignorer l'authentification IdP et de naviguer directement vers l'instance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Cette erreur se produit lorsque l'instance ne fournit pas à ADFS la définition et la sémantique nécessaires pour l'attribut SPNameQualifier dans SAMLResponse.

Activez l'authentification initiée par le fournisseur de service en effectuant l'une des actions suivantes :

Procédure

- Effectuez une mise à niveau vers SAML 2.0 Update 1 et désactivez l'option de création d'une demande AuthnContextClass.
- Modifiez l'include de script **SAML2** pour commenter les définitions de l'attribut SPNameQualifier lorsque SAML 2.0 est actif (et non SAML 2.0 Update 1).

  Commentez ces lignes dans les fonctions createNameID et createNameIDPolicy :

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

Que faire ensuite
Si vous ne souhaitez pas que l'invite de connexion de votre serveur ADFS s'affiche lorsque vous accédez à l'instance, définissez la propriété SAML 2.0 Update 1 suivante sur false : **Créez une demande AuthnContextClass dans l'instruction AuthnRequest** (`glide.authenticate.sso.saml2.createrequestedauthncontext`).

(Solution de contournement) Prendre en charge l'authentification Kerberos

Une solution de contournement est disponible pour l'intégration SAML 2.0 qui modifie le contexte d'authentification de l'authentification basée sur des formulaires à l'authentification basée sur Windows.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Actuellement, l'intégration SAML 2 utilise un contexte d'authentification PasswordProtectedTransport ou « authentification basée sur les formulaires ». Ce contexte d'authentification exige que l'IdP présente aux utilisateurs un formulaire pour les informations d'identification d'authentification. Avec Kerberos, une session SAML est déjà active via une connexion Windows établie, de sorte que l'utilisateur n'a pas besoin de s'authentifier avec l'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Ouvrez l'enregistrement **IdP SAML2 Update1** .
3. Définissez la **méthode AuthnContextClassRef que nous inclurons dans notre SAML 2.0 AuthnRequest au fournisseur d'identité** sur l'une des options suivantes :

Valeurs de la méthode AuthnContextClassRef
urn :oasis :names :tc :SAML :2.0 :ac :classes :PasswordProtectedTransport (par défaut)
urn :federation :authentication :windows

4. Cliquez sur **Mettre à jour**.

Intégration d'Azure AD à SAML 2.0

Intégrez ServiceNow à Azure Active Directory (Azure AD).

L'intégration ServiceNow à Azure AD vous permet d'effectuer les actions suivantes :

- Contrôle dans Azure AD qui a accès à ServiceNow.
- Permettez aux utilisateurs de se connecter ServiceNow automatiquement avec leurs comptes Azure AD.
- Gérez vos comptes dans le portail Azure.

Conditions préalables

Pour commencer, vous devez effectuer les opérations suivantes :

- Un abonnement Azure AD. Si vous n'avez pas d'abonnement, vous pouvez obtenir un compte gratuit.
- Authentification ServiceNow unique (SSO) activée.
- Une ServiceNow instance ou un ServiceNow locataire qui prend en charge les versions San Diego ou ultérieures.
- Le module d'extension Authentification unique de plusieurs fournisseurs doit être activé pour un ServiceNow locataire.
- Pour une configuration automatique, activez le module d'extension multi-fournisseurs pour ServiceNow.

Ensemble d'actions pour la configuration

Voici l'ensemble des actions qui doivent être effectuées pour configurer Azure AD :

- Ajouter ServiceNow à partir de la galerie à Azure AD.
- Configurer Azure AD SSO
- Créer un utilisateur de test Azure AD
- Affecter l'utilisateur de test Azure AD
- Configurer ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter ServiceNow à partir de la galerie

Ajoutez ServiceNow à partir de la galerie à votre liste d'applications SaaS managées sur Azure AD.

Avant de commencer

Rôle requis : administrateur Azure

Procédure

1. Connectez-vous au portail Azure à l'aide d'un compte Microsoft.
2. Sélectionnez le service **Azure Active Directory** dans le volet de gauche.
3. Accédez à la **Applications d'entreprise** > **Toutes les applications**.
4. Pour ajouter une nouvelle application, sélectionnez **Nouvelle** application.
5. Dans la section Ajouter à partir de la galerie, entrez ServiceNow dans la zone de recherche.
6. Sélectionnez ServiceNow dans le panneau des résultats, puis ajoutez l'application.
7. Patientez quelques secondes pendant que l'application est ajoutée à votre locataire.

Configurer Azure AD SSO

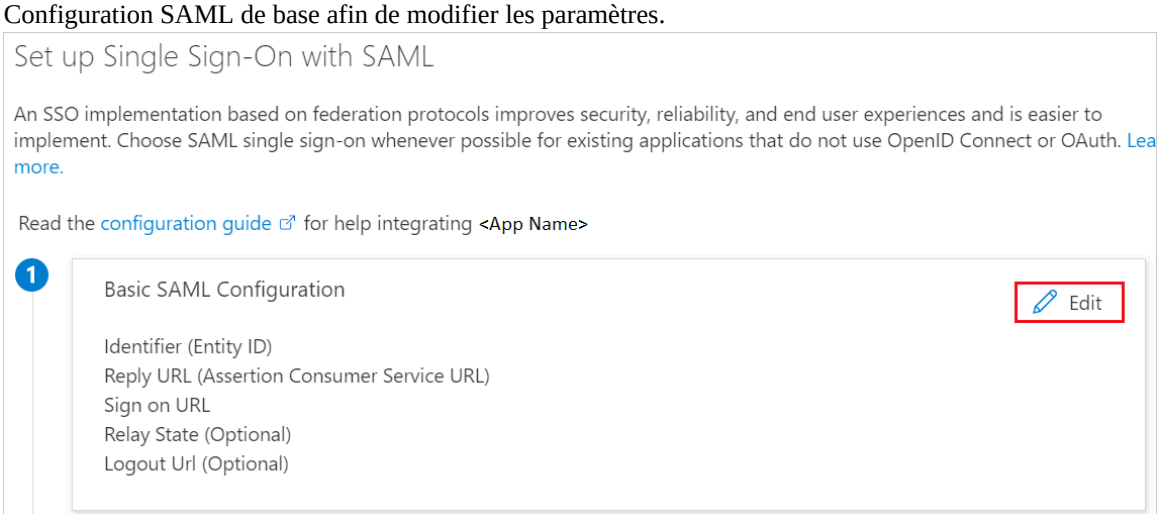
Configurez Azure AD SSO dans le portail Azure.

Avant de commencer

Rôle requis : administrateur Azure

Procédure

1. Sur la page d'intégration de l'application ServiceNow du portail Azure, recherchez la section Gérer.
2. Sélectionnez l'authentification unique.
   Sur la page Sélectionner une méthode d'authentification unique, sélectionnez SAML.
3. Sur la page Configurer l'authentification unique avec SAML, sélectionnez l'icône en forme de stylo pour Configuration SAML de base afin de modifier les paramètres.



4. Dans la section Configuration SAML de base, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans **URL de connexion**, saisissez l'un des modèles d'URL suivants :

```
https://<instancename>.service-now.com/navpage.do
https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Remarque :
Vous devez fournir le sys_id dans cette URL.

b. Dans Identificateur (ID d'entité), saisissez une URL avec le modèle : `https://<nom-instance>.service-now.com`.

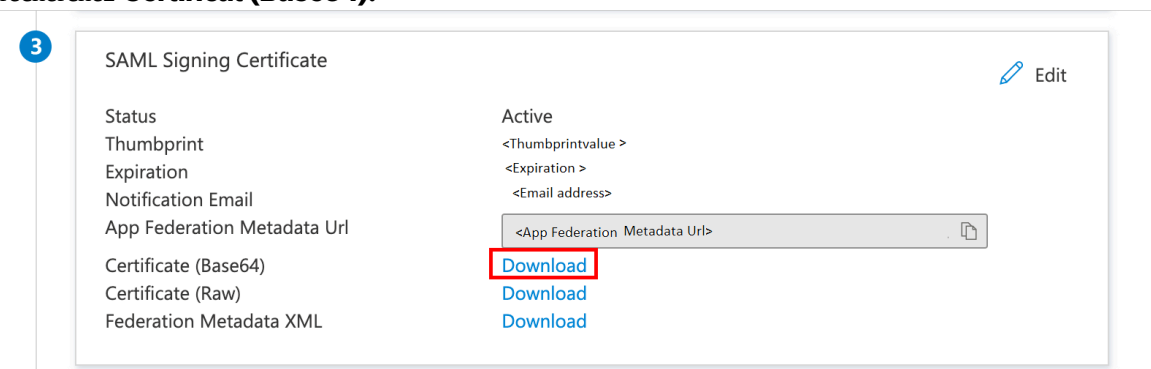
c. Pour **URL de réponse**, entrez l'un des modèles d'URL suivants :

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Dans URL de déconnexion, entrez une URL avec le modèle : `https://<instancename>.service-now.com/navpage.do`

Remarque :
Vous devez mettre à jour l'URL d'ouverture de session, l'URL de réponse, l'URL de déconnexion et l'identificateur. les valeurs indiquées dans ces URL sont à des fins de démonstration.

5. Sur la page Configurer l'authentification unique avec SAML, dans la section Certificat de signature SAML, recherchez **Certificat (Base64).**



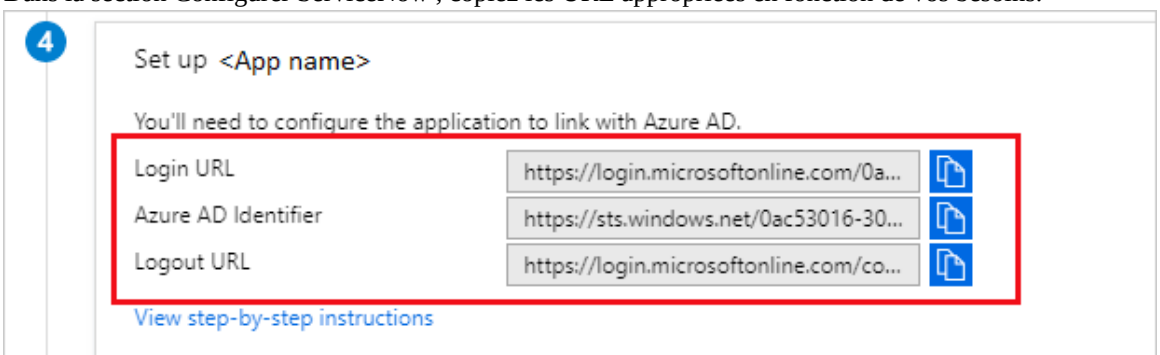
a. Sélectionnez le bouton Copier pour copier **l'URL des métadonnées d'App Federation** et collez-la dans le Bloc-notes.
Cette URL est requise pour la configuration ultérieure.

b. Sélectionnez **Télécharger** pour télécharger le certificat (Base64).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la section Configurer ServiceNow , copiez les URL appropriées en fonction de vos besoins.



Créer un utilisateur de test Azure AD

Créez un utilisateur test sur Azure AD.

Avant de commencer
Rôle requis : administrateur Azure

Procédure

1. Sur le portail Azure, accédez à **Tous** > **Azure Active Directory** > **Utilisateurs** > **Tous les utilisateurs**.
2. Sélectionnez **Nouvel utilisateur**.
3. Dans les propriétés utilisateur, fournissez les informations suivantes :
   - Nom
   - Nom d'utilisateur
   - Mot de passe
4. Cliquez sur **Créer**.

Affecter l'utilisateur de test Azure AD

Affectez l'utilisateur de test Azure AD créé pour utiliser l'authentification unique Azure en lui accordant l'accès à ServiceNow.

Avant de commencer
Rôle requis : administrateur Azure

Procédure

1. Sur le portail Azure, accédez à **Tous** > **Applications d'entreprise** > **Toutes les applications**.
2. Dans la liste des applications, sélectionnez ServiceNow.
3. Sur la page de l'application, dans la section Gérer, sélectionnez **Utilisateurs et groupes**.
4. Sélectionnez **Ajouter un utilisateur**.
5. Dans la fenêtre **Ajouter une affectation** , sélectionnez **Utilisateurs et groupes**.
6. Dans la fenêtre **Utilisateurs et groupes** , sélectionnez l'utilisateur test qui a été créé dans la liste des utilisateurs.
7. Choisissez le rôle de l'utilisateur affecté dans la liste **déroulante Sélectionner un rôle** si nécessaire.
8. Dans la fenêtre **Ajouter une affectation** , sélectionnez **Affecter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer ServiceNow

Configurez ServiceNow avec les détails Azure AD pour utiliser SSO.

Avant de commencer

Module d'extension : Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs

Activez les propriétés SSO de plusieurs fournisseurs :

- Sélectionnez **Activer l'authentification unique (SSO) de plusieurs fournisseurs**.
- Sélectionnez **Activer l'importation automatique d'utilisateurs à partir de tous les fournisseurs d'identité dans la table utilisateur**.
- Sélectionnez **Activer la journalisation du débogage pour l'intégration de l'authentification unique (SSO) de plusieurs fournisseurs**.
- Saisissez **une adresse e-mail**, champ de la table utilisateur qui .....

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sur la page Fournisseurs d'identité, sélectionnez **Nouveau**.
3. Dans la fenêtre Fournisseurs d'identité, sélectionnez **SAML**.
4. Dans la section Importer les métadonnées du fournisseur d'identité, vous pouvez soit :
   - **URL** : URL des métadonnées App Federation pour renseigner automatiquement les détails sur la page de configuration du fournisseur d'identité.
   - **Importer** : importez le code XML pour importer les détails sur la page de configuration du fournisseur d'identité.
5. Cliquez avec le bouton droit en haut de l'écran, cliquez sur **Copier sys_id** et utilisez cette valeur dans la section **URL de connexion** dans la configuration **SAML de base** .
6. Remplissez les champs du formulaire.

Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	Nom du fournisseur d'identités. Cet IdP est l'ID système de redirection automatique.
Actif	Oui	Actif doit être défini sur vrai pour que l'IdP soit utilisé pour l'authentification. **Remarque :** L'option permettant de définir cette propriété n'intervient qu'après un test de la connexion réussi.
Par défaut	Non	L'IdP de redirection automatique, anciennement appelé fournisseur d'identités primaire, redirige automatiquement les utilisateurs vers l'URL de l'instance de base. Cette propriété définit cette configuration IdP par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

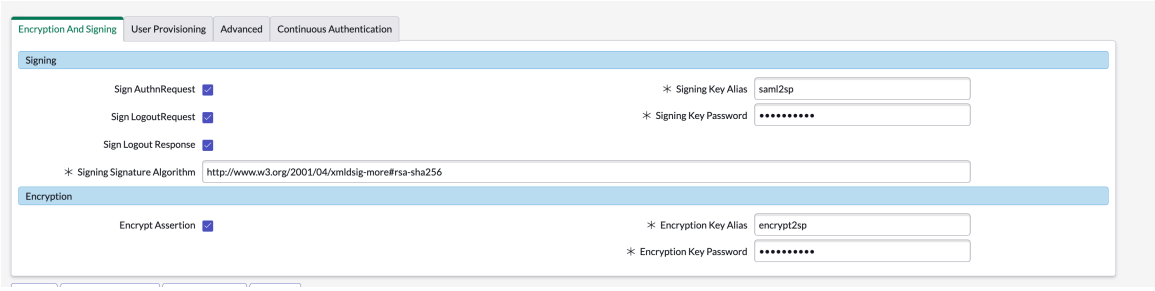
Propriété	Obligatoire	Description
Rediriger automatiquement l'IdP	Non	Configuration IdP que vous pouvez définir comme IdP de redirection automatique. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est mis à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système, automatiquement activée, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	URL de votre fournisseur d'identité. Chaque URL IdP doit être unique.
Service AuthnRequest du fournisseur d'identité	Oui	URL vers la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService.
Service SingleLogoutRequest du fournisseur d'ident	Non	URL obtenue à partir de l'élément SingleLogoutService.
ServiceNow Page d'accueil	Oui	URL, y compris la page de connexion, de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/navpage.do
ID d'entité/émetteur	Oui	URL de base, à l'exclusion de la page de connexion de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
URI de l'audience	Oui	URL de base, à l'exclusion de la page de connexion de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
Politique NameID	Oui	Valeur de l'élément NameIDFormat que l'intégration utilise.
Redirection de déconnexion externe	Non	URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion.
Échec de la redirection du besoin	Non	URL de redirection des demandes d'authentification ayant échoué. Par défaut, il s'agit du point de terminaison d'URL d'une page d'erreur ou d'une page de déconnexion configurée dans l'IdP. Vous pouvez renseigner cette valeur dans le champ glide.authenticate.failed_requirement_redirect.

7. **Facultatif :** Onglet Chiffrement et signature

Remarque :
Utilisez vos propres certificats pour le chiffrement et la signature.

Traduction automatique

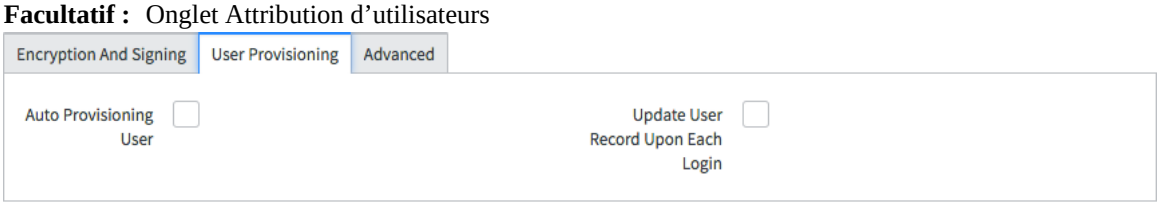
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champs de chiffrement et de signature

Propriété	Description
Alias de la clé de signature/ chiffrement	Alias de l'entrée de clé stocké dans le magasin de clés SAML 2.0 SP.
Signature avec le mot de passe de clé	Mot de passe de l'entrée de clé stocké dans le magasin de clés SAML 2.0 SP.
Chiffrer l'assertion	Case à cocher pour chiffrer l'assertion dans la réponse SAML. Les métadonnées générées pour l'IDP incorporent le certificat x509, que l'IDP utilise pour chiffrer l'assertion dans la réponse SAML qu'il génère.
Algorithme de signature pour la signature	URL qui pointe sur le consommateur AuthnRequest du fournisseur d'identité SAML 2.0 pour l'authentification de signature électronique.
Signer l'AuthnRequest	Case à cocher pour activer le service d'authentification unique IdP pour recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Case à cocher pour activer le service d'authentification unique IdP pour recevoir une LogoutRequest.

8. **Facultatif :** Onglet Attribution d'utilisateurs



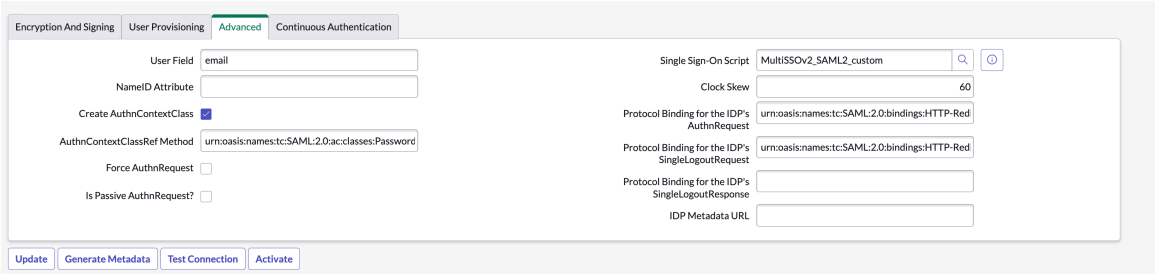
Champs d'attribution d'utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	La mise en service automatique d'utilisateurs crée les utilisateurs lorsque l'utilisateur n'existe pas dans la table des utilisateurs de l'instance sur la base des informations fournies par l'IdP.
Mettre à jour l'enregistrement utilisateur à chaque connexion	Mettre à jour les informations utilisateur dans la table Utilisateur de l'instance avec les informations dans l'IdP chaque fois que l'utilisateur se connecte à l'aide de SAML.

9. **Facultatif :** Onglet Avancé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champs avancés

Propriété	Description
Champ d'utilisateur	Champ de la table Utilisateur qui contient la valeur que l'IdP nécessite pour identifier l'utilisateur. Cet ID unique fait partie de la réponse. Par exemple, un nom d'utilisateur, un ID d'employé, etc. Dans la table utilisateur système, cet ID unique est mis en correspondance avec les détails de l'utilisateur.
Attribut NameID	Champ que vous laissez vide sauf si vous configurez une nouvelle politique NameID. Si vous configurez une nouvelle politique, le système nécessite la table Utilisateur qu'il doit utiliser pour identifier l'utilisateur qui se connecte. Le système associe le jeton NameID au nom de ce champ de table Utilisateur.
Créer une AuthnContextClass	Case à cocher pour spécifier une classe de contexte particulière, telle que Transport protégé par mot de passe. Si la case n'est pas cochée, l'IdP sélectionne la classe de contexte la plus appropriée.
Méthode AuthnContextClassRef	URN du mécanisme de connexion que vous souhaitez que l'IdP utilise pour authentifier les utilisateurs.
Forcer l'AuthnRequest	Case à cocher permettant de forcer l'exécution d'AuthnRequest.
Est une AuthnRequest passive	Cochez la case si l'AuthnRequest est passive.
Script d'authentification unique	Script d'authentification unique. La valeur par défaut est *MultiSSOV2_SAML2_custom*.
Signer la réponse de déconnexion	Détails de la réponse de déconnexion dans ce champ.
Décalage d'horloge	Nnombre de secondes entre les deux attributs qui composent le nonce de la réponse SAML. La valeur par défaut est 60. Une SAMLResponse valide doit se situer entre les valeurs *date-heure notBefore* et *notOnOrAfter* . Voir Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour un exemple de message SAMLResponse.
Protocole de liaison du service SingleLogoutReuqest de l'IDP	L'une des valeurs prises en charge répertoriées dans l'attribut Binding de l'élément SingleLogoutService.
URL des métadonnées à partir de laquelle les propriétés IDP sont importées	Les propriétés IdP sont importées à partir de cette URL. Si activé, il active l'importation automatique du certificat SAML à partir de l'IdP si le certificat précédent a expiré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : Si vous effectuez une mise à niveau de SAML2 Update 1 vers l'authentification unique (SSO) de plusieurs fournisseurs ou si vous configurez manuellement votre connexion SSO, l'URL des métadonnées IdP n'est pas automatiquement renseignée.
Demande	ID unique dans le cadre de la demande. L'ID peut être un nom d'utilisateur, un ID d'employé, etc. **Remarque :** La redirection et la liaison de publication sont toutes deux prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après un test de la connexion réussi. Pour plus d'informations, consultez Tester les connexions IdP.
Réponse	ID unique dans le cadre de la réponse. L'ID peut être un nom d'utilisateur, un ID d'employé, etc. **Remarque :** La redirection et la liaison de publication sont toutes deux prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après un test de la connexion réussi. Pour plus d'informations, consultez Tester les connexions IdP.

10. Sélectionnez **Test de la connexion** dans le coin supérieur droit de la page.
11. Entrez vos informations d'identification.
    Les résultats des tests de déconnexion de l'authentification unique s'affichent.
12. Sélectionnez **Activer** pour activer la configuration.

Liens d'e-mail avec authentification externe

Vous pouvez utiliser des liens d'e-mail lors de l'utilisation de l'authentification externe de jeton digestif, mais vous devez déterminer comment gérer les liens dans les notifications par e-mail.

Les liens par défaut contiennent une URL qui vous dirige vers un emplacement spécifique dans l'instance, comme un incident ou une demande de changement, sans intégrer les informations d'identification SSO. Vous trouverez ci-dessous des exemples permettant de diriger l'utilisateur vers l'emplacement dans l'instance sans se connecter à la page de connexion de l'instance.

- Technique HTTP non chiffrée pour se connecter à l'instance /demo (elle ne navigue pas vers un enregistrement spécifique) :

```
https://<instance
 name>.service-now.com/?
SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

- Lier (dans une notification par e-mail) à un enregistrement spécifique, afin que l'utilisateur accède d'abord au portail de connexion de l'entreprise :

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez définir la `glide.email.override.url` propriété dans votre instance pour qu'elle contienne l'URL de la page du portail de la société. Si cette propriété n'existe pas, vous pouvez la créer.

- Le portail d'entreprise doit ensuite prendre cette URL et construire l'URL de redirection vers l'instance en préservant le segment nécessaire pour accéder à l'enregistrement spécifique, et en ajoutant les informations d'identification SSO à la fin de l'URL :

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb0942
23466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_
name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24tbE=
```

Ajouter la prise en charge de la signature électronique pour SAML

Configurez les propriétés suivantes pour la signature électronique avec le langage de balisage d'assertion de sécurité (SAML) 2.0 mise à jour 1.

Lorsque la signature électronique est active avec l'authentification unique (SSO), les propriétés SAML ne sont pas utilisées. Le système ajoute des propriétés de signature électronique à la table Propriétés SAML2 Update1 [saml2_update1_properties] :

Propriété	Description	Par défaut
Index de consommateur d'assertion pour l'authentification de signature électronique	Numéro d'index qui identifie le point de terminaison.	1
URL de consommateur d'assertion pour l'authentification de signature électronique	URL qui identifie le consommateur.	`https://yourinstance.service-now.com/consumer.do`
URL AuthnRequest pour l'authentification de signature électronique	URL d'authentification	aucun

Si vous utilisez la signature électronique avec SAML 1.0 ou SAML 2.0 (à l'exception de la mise à jour 1), consultez les instructions de configuration spéciales : Signature électronique pour l'authentification unique (SSO) de plusieurs fournisseurs.

Remarque :
Si vous êtes un client des sciences de la vie utilisant la signature électronique, désactivez la règle métier Prévention du verrouillage automatique de l'utilisateur.

Migration d'une intégration SAML 1.1 existante vers SAML 2.0

Pour migrer d'une intégration SAML 1.1 à une intégration SAML 2.0, contactez l'assistance clientèle.

Mettre à jour votre intégration SAML 2.0 existante

Mettez à jour votre intégration SAML 2.0 existante.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Demandez le module d'extension SAML 2.0 Update 1. Contact Service client et assistance pour demander le module d'extension *SAML 2.0 Single Sign-On - Update 1 : security enhancements* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module d'extension applique les versions mises à jour de la sortie d'installation *SAML2SingleSignon* (script de connexion), de la sortie d'installation *SAML2Logout* (script de déconnexion) et de *l'include de script SAML2* (objet de script).

Fusionner les personnalisations des scripts de sortie d'installation existants dans de nouveaux scripts. La mise à jour enregistre une copie inactive des scripts de sortie d'installation d'origine de l'intégration. Vous pouvez utiliser ces copies pour fusionner toutes les personnalisations que vous avez apportées aux scripts de connexion et de déconnexion aux nouvelles versions de ces sorties d'installation.

Fusionner les personnalisations à partir de scripts de sortie d'installation existants dans de nouveaux scripts

Nom du script de sortie de l'installation d'origine	État du script original	Nom du script de sortie de nouvelle installation	Statut du nouveau script
SAML2SingleSignon	Inactif	SAML2SingleSignon_update1	Actif
SAML2	Inactif	SAML2_update1	Actif
SAML2Déconnexion	Inactif	SAML2Logout_update1	Actif

Vous pouvez accéder aux scripts de sortie d'installation et de déconnexion SAML 2.0 en utilisant les chemins suivants :

- **Authentification unique SAML 2** > **Script de connexion**.
- **Authentification unique SAML 2** > **Script de déconnexion**.
- **Définition du système** > **Sorties d'installation**.

Vous pouvez accéder à l'include de script SAML 2.0 mise à jour 1 en utilisant les chemins d'accès suivants :

- **Authentification unique SAML 2** > **Objet de script**.
- **Définition du système** > **Includes de script**.

Testez la mise à jour.

Procédure

1. Ajoutez une propriété système appelée `glide.authenticate.sso.saml2.debug avec la` valeur *vrai*.
2. Tentative de connexion SAML 2.0.
3. Examinez le journal système.
   Les erreurs de validation SAML2 commencent par le texte *SAML2ValidationError*.
4. Identifiez et corrigez les erreurs de connexion courantes.
   Pour plus d'informations, consultez Erreurs et correctifs Multi-SSO (SAML 2.0).

Exemples de réponses SAML 2 après la mise à jour

Les sections suivantes illustrent les nouveaux éléments et attributs requis que l'IdP doit fournir dans la réponse SAML.

Exemple de réponse SAML 2 avec élément d'émetteur

La réponse SAML 2 suivante utilise l'élément *Émetteur* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData

La réponse SAML 2 suivante utilise les éléments *SubjectConfirmation* et *SubjectConfirmationData* avec les attributs *NotOnOrAfter* et *Recipient* .

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:Subject
ConfirmationData InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience

La réponse SAML 2 suivante utilise les éléments *AudienceRestrictions* et *Audience* avec les attributs *NotBefore* et *NotOnOrAfter* .

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```

Attribution d'utilisateurs SAML

Si des utilisateurs existent dans votre IdP mais ne sont pas dans votre instance, la mise en service des utilisateurs SAML peut créer automatiquement les utilisateurs dans la table Utilisateur [sys_user] de votre instance.

La mise en service d'utilisateurs SAML est prise en charge pour SAML 2.0 Update 1 lorsque la SSO à fournisseurs multiples est activée.

Fonctionnement de l'attribution d'utilisateurs SAML

Lorsque la mise en service d'utilisateurs SAML est activée et que le système rencontre un nouvel utilisateur qui n'est pas dans l'instance, l'instance crée automatiquement un enregistrement dans une table temporaire avec le nom `u_imp_saml_user_<suffixe>`, où `<suffixe>` est un identificateur de texte généré automatiquement. Le système crée également une carte de transformation qui spécifie les relations de données entre la table d'importation et la table utilisateur. Chaque IdP identifié dans le système possède sa propre carte de transformation. La carte de transformation est créée une fois pour chaque IdP. Les administrateurs peuvent le mettre à jour si nécessaire.

Lorsque l'utilisateur se connecte, il accède à un IdP pour se connecter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le système présente une liste de tous les fournisseurs d'identités qui sont en mesure d'utiliser la mise en service d'utilisateurs SAML. S'il n'y a qu'un seul IdP qui peut utiliser la mise en service d'utilisateurs SAML, celui-ci est utilisé automatiquement.
- Si aucune des conditions ci-dessus n'est vraie, le système utilise l'IdP de redirection automatique.

Administrer la mise en service des utilisateurs SAML

Mettez à jour la table Utilisateur avec les utilisateurs de votre IdP en configurant d'abord le mappage de champs, puis en activant la mise en service d'utilisateurs via les paramètres d'IdP à SSO de fournisseurs multiples.

Avant de commencer

Configurez votre mappage d'IdP pour identifier les champs de l'IdP qui sont mappés aux champs corrects de la table Utilisateur.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Propriétés**.
2. Sélectionnez **Activer l'importation automatique d'utilisateurs à partir de tous les fournisseurs d'identité dans la table utilisateur** (`glide.authenticate.multisso.user.autoprovision`) pour activer cette fonctionnalité.
3. Cliquez sur **Enregistrer**.
4. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
5. Ouvrez l'enregistrement Fournisseur d'identité que vous souhaitez utiliser.
6. Créez un enregistrement dans la table Utilisateur si l'utilisateur n'existe pas déjà en sélectionnant **Mettre en service automatiquement les utilisateurs**.
   Si vous avez effectué une mise à niveau vers cette version, vous devez configurer le formulaire et ajouter ce champ.
7. Autorisez la mise à jour des enregistrements utilisateur lorsque les utilisateurs se connectent à l'IdP et que les informations sur l'IdP ne sont pas à jour par rapport aux informations de la table Utilisateur en sélectionnant **Mettre à jour l'enregistrement utilisateur à chaque connexion**.
   Si vous avez effectué une mise à niveau vers cette version, vous devez configurer le formulaire et ajouter ce champ.
8. Cliquez sur **la carte de transformation de l'attribution d'utilisateurs** pour afficher la carte créée automatiquement par le système.
9. Apportez des modifications à la carte selon vos besoins.

Résultats

Lorsque les premiers utilisateurs inconnus tentent de se connecter, le système crée les champs de la table de jeu d'importation à partir du fichier metadata.xml.

Remarque :
Vous ne pouvez pas mapper les champs à partir de la table IdP tant que ce premier utilisateur ne s'est pas connecté.

Dépannage SAML 2.0

Avant de contacter le support, essayez les solutions de dépannage disponibles dans la base de connaissances sur Hi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
L’instance ne prend pas en charge les solutions fournies par des sites externes.

Consultez l’article de la base de connaissances suivant : KB0540617 "Matrice d’erreurs SAML".

Autres problèmes courants

Erreur ou symptôme	Solution
Message d’erreur : « n’est pas une fonction ». Ce problème peut se produire dans un environnement à plusieurs nœuds. Si le module d’extension n’est pas activé sur tous les nœuds, une erreur comme celle-ci s’affiche : org.mozilla.javascript.EcmaError : `[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]` n’est pas une fonction.	Cette erreur se produit car le module d’extension n’était pas actif et n’a pas chargé le fichier .jar. Par conséquent, le code semble manquer. Contactez l’assistance technique pour redémarrer les nœuds auxquels le module d’extension est manquant.
SAML n’authentifie pas les utilisateurs accédant aux pages CMS.	Par défaut, les pages CMS sont publiques et ne nécessitent donc pas d’authentification. Si vous souhaitez que SAML authentifie les pages CMS, changez la page publique *view_content.do* de *active=true* à *active=false*.
Impossible de rediriger un utilisateur vers une page CMS après l’authentification SAML.	Par défaut, l’intégration SSO utilise un paramètre d’URL appelé *URI* pour contrôler où l’utilisateur est dirigé après l’authentification au niveau du fournisseur d’identités. L’authentification unique ignore les URL relatives. Par exemple, SSO ne peut pas rediriger les utilisateurs vers une URL relative */ess* . Au lieu de cela, l’utilisateur doit naviguer vers une URL telle que */nav_to.do ?uri=/ess*, qui utilise la syntaxe de lien profond. Cependant, cela place le portail ESS dans l’IFrame de contenu de navigation principal. En d’autres termes, le site n’occupe pas la page complète, mais se charge plutôt comme une page dans votre instance. Pour plus d’informations, consultez Sites CMS et Single Sign-On. Si vous modifiez la page d’entrée CMS pour la rendre privée en définissant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autres problèmes courants (suite)

Erreur ou symptôme	Solution
	view_content.do sur *active=false*, le comportement de lien profond nécessite alors une personnalisation du script de connexion de *sortie d'installation* . Créez un script qui recherche la partie *URI* de l'URL et construit un paramètre d'URL *RelayState* contenant le chemin de l'URL relative pour rediriger les utilisateurs après authentification auprès du fournisseur d'identités.
SAML ne redirige pas les utilisateurs vers la page appropriée après l'authentification.	Déterminez si l'état du relais est transmis à l'IdP, puis renvoyé pendant l'authentification. Vous pouvez le faire avec un navigateur capable d'enregistrer les en-têtes de requête HTTP et les informations POST, tel que Chrome avec ses outils de développement intégrés, ou Firefox avec le module complémentaire appelé HTTPfox. Pour Internet Explorer, utilisez une application tierce telle que Fiddler. L'objectif est de voir les requêtes passer du client (navigateur) à l'instance, et du client à l'IdP.

Surveiller la file d'attente de l'événement pour les activités de connexion

Chaque intégration d'authentification crée des événements pour les activités de connexion.

Vous pouvez utiliser ces événements pour surveiller les échecs de connexion et déterminer s'il existe des problèmes de sécurité à résoudre.

Surveillance de la file d'attente de l'événement pour les échecs de connexion

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
`external.authentication.succeeded`	L'authentification externe a réussi et l'utilisateur a accédé à l'URL d'instance.	ID de session	ID d'utilisateur de l'utilisateur qui s'est connecté avec succès	URL à laquelle l'utilisateur a accédé (qui peut être un lien profond)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Surveillance de la file d'attente de l'événement pour les échecs de connexion (suite)

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
external.authentication.failed	Les exigences d'authentification unique ne sont pas présentes ou sont manquantes.		ID de session	Les exigences d'authentification manquantes
external.authentication.failed	L'utilisateur n'existe pas dans la table Utilisateur [sys_user]		ID d'utilisateur	La chaîne « L'utilisateur n'existe pas »
external.authentication.failed	L'utilisateur est verrouillé.		ID d'utilisateur	La chaîne « Utilisateur verrouillé ».

Événements de connexion à la file d'attente de l'événement

L'intégration SAML 2.0 crée des événements pour les activités de connexion.

Vous pouvez utiliser ces événements pour surveiller les échecs de connexion et déterminer s'il existe des problèmes de sécurité à résoudre.

Événements d'activités de connexion

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
SAML2.Déconnexion.Validation.Échec	La réponse de déconnexion de l'IdP a échoué à la validation de votre demande de déconnexion. L'événement valide l'élément <inResponseTo> par rapport à l'ID de session (attribut ID de l'élément <saml2p :LogoutRequest>). Par exemple, consultez le workflow pour la demande de déconnexion émise.	ID de session	La chaîne « Échec de la validation de la réponse de déconnexion SAML2 ».
authentification.externe.réussie	Authentification externe réussie.		La chaîne « Authentification réussie »
authentification.externe.réussie	L'authentification externe a réussi et l'utilisateur a accédé à l'URL d'instance.	ID de session et ID d'utilisateur de l'utilisateur qui s'est connecté avec succès	URL à laquelle l'utilisateur a accédé (qui peut être un lien profond)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Événements d'activités de connexion (suite)

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
Échec.authentification.externe	Les exigences d'authentification unique ne sont pas présentes ou sont manquantes.	ID de session	Les exigences d'authentification manquantes
Échec.authentification.externe	L'utilisateur n'existe pas dans la table Utilisateur [sys_user].	ID d'utilisateur	La chaîne « L'utilisateur n'existe pas »
Échec.authentification.externe	L'utilisateur est verrouillé.	ID d'utilisateur	La chaîne « Utilisateur verrouillé »

Authentification entrante et sortante OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance sur le système à l'aide d'un protocole d'authentification.

OAuth 2.0 : autorisation ouverte est le protocole d'autorisation standard de l'industrie, qui s'appuie sur la simplicité des développeurs clients tout en fournissant des flux d'autorisation spécifiques pour les applications Web, les applications de bureau et les équipements mobiles.

Il s'agit d'une norme conçue pour permettre à un site web ou à une application d'accéder à des ressources hébergées par d'autres applications web au nom d'un utilisateur.

Au lieu d'utiliser les informations d'identification de l'utilisateur de ressource pour accéder aux ressources protégées, le client obtient un jeton d'accès. Les jetons d'accès sont émis aux clients tiers avec l'approbation de l'utilisateur, qui utilise ensuite le jeton d'accès pour accéder aux ressources protégées.

Depuis Zurich, vous pouvez configurer l'intégration OAuth avec les améliorations suivantes :

- Augmentez la longueur du secret client à 2 048 caractères pour répondre aux exigences de sécurité des systèmes tiers tels qu'Azure DevOps (ADO).
- Fournissez une URL JSON Web Key Set (JWKS) pour gérer et mettre à jour automatiquement la clé publique pour la validation de signature des jetons Web JSON (JWT).
- Demandez des jetons OAuth à l'aide du type d'accord JWT signé avec des algorithmes de sécurité renforcée (ES).
- Configurez un identificateur unique pour les jetons JWT.

Entrant

Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client dont le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section Entrant OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sortant

Utilisez un fournisseur OAuth tiers qui fournit l'autorisation d'accès à votre instance. Spécifiez un profil OAuth et un périmètre OAuth lorsque vous vous connectez à un autre fournisseur OAuth. Pour plus d'informations, reportez-vous à la section Sortant OAuth.

OAuth 2.0

OAuth 2.0 permet aux utilisateurs d'accéder aux ressources d'instance via des clients externes en obtenant un jeton plutôt qu'en saisissant des informations d'identification de connexion à chaque demande de ressource.

Vous devez disposer du rôle security_admin pour gérer l'intégration OAuth. Configurez OAuth 2.0 pour les scénarios suivants :

- **Scénario de client externe OAuth** (entrant) : votre instance fournit un point de terminaison permettant aux clients tiers d'extraire des données de l'instance.
- **Scénario du fournisseur OAuth** (sortant) : votre instance extrait les données d'un fournisseur tiers.

Remarque :
Vous devez vous authentifier pour la première fois pour récupérer la publication du jeton, ce que vous n'avez pas besoin d'authentifier à l'aide d'un compte utilisateur avant l'expiration du jeton.

Les frameworks de sécurité simple et haute sécurité prennent en charge OAuth 2.0. Une haute sécurité est recommandée. Consultez pour plus d'informations sur les versions dans lesquelles la haute sécurité est déjà active et sur la façon d'activer la haute sécurité.

Concepts clés de l'implémentation d'OAuth 2.0

Concept	Description
Propriétaire de ressource	Entité capable d'accorder l'accès à une ressource protégée. Un propriétaire de ressource qui est une personne est appelé utilisateur *final*. Le propriétaire de ressource est toujours un compte utilisateur.
Client	Application qui, avec l'autorisation du propriétaire de la ressource, effectue des demandes de ressources protégées au nom du propriétaire de la ressource.
Serveur de ressources	Serveur qui héberge les ressources protégées, capable d'accepter les demandes de ressources protégées et d'y répondre.
Serveur d'autorisation	Serveur qui émet des jetons d'accès au client après avoir authentifié le propriétaire de ressource et obtenu l'autorisation.
Demande d'autorisation	Autorisation dont un client a besoin pour accéder à une ressource protégée. La demande d'autorisation est toujours un message HTTP POST contenant l'ID du client qui agit au nom du propriétaire de ressource et les informations d'identification qui autorisent la demande.
Octroi d'autorisation	Informations d'identification qui représentent l'autorisation du propriétaire de la ressource d'accéder à une ressource. L'autorisation est accordée sous forme d'informations d'identification de connexion de l'utilisateur ou d'un jeton de rafraîchissement.
Jeton d'accès	Chaîne sécurisée qu'un client utilise pour accéder aux ressources protégées. Une instance émet des jetons d'accès aux clients qui disposent d'une autorisation valide. Chaque jeton d'accès a un champ d'application, une durée de vie et d'autres attributs spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Concept	Description
	Par défaut, une instance émet des jetons d'accès d'une durée de vie de 30 minutes dans le scénario où l'instance est le fournisseur OAuth. Pour les jetons tiers, 30 jours.
Actualiser le jeton	Informations d'identification qu'un client utilise pour obtenir de nouveaux jetons d'accès sans nécessiter d'autorisation utilisateur supplémentaire. Une instance émet un jeton d'actualisation à un client lorsqu'elle est autorisée pour la première fois à disposer d'un jeton d'accès. Par défaut, une instance émet des jetons d'actualisation avec une durée de vie de 100 jours dans le scénario où l'instance est le fournisseur OAuth. Pour les jetons tiers, 365 jours.
Certificats auto-signés	La ne prend pas en charge les ServiceNow AI Platform certificats auto-signés. Le client OAuth n'utilise pas le magasin de clés de confiance de certificat et n'autorise pas la connexion aux points de terminaison OAuth qui intègrent un certificat auto-signé.
Agent utilisateur	Utilisateur qui délègue les droits d'accès à une application cliente, souvent un site web. Les droits d'accès permettent à l'application cliente ou au site Web d'accéder aux données dans l'instance à laquelle l'utilisateur a des droits d'accès. L'agent utilisateur est utilisé dans le scénario.

Types d'accords OAuth

Un *type d'accord* est la façon dont le client obtient le jeton d'accès. Les types d'octroi suivants sont pris en charge :

- **Code d'autorisation** : le consommateur obtient d'abord un code d'autorisation, puis l'utilise pour obtenir un jeton d'accès. Vous pouvez spécifier un profil OAuth et spécifier ce type d'accord. Le processus qui utilise le code d'autorisation est également appelé *flux de code d'authentification* ou *flux de code d'autorisation*.
- **Informations d'identification du mot de passe du propriétaire de ressource** : le consommateur de la ressource dispose déjà des informations d'identification de l'utilisateur pour obtenir le jeton d'accès. Ce processus est également appelé flux de *mots de passe*.
- **Informations d'identification du client** : le consommateur de la ressource utilise l'ID client et le secret client qui sont déjà configurés dans le registre d'application.

Stockage des informations d'identification d'authentification

Le secret client OAuth est stocké en tant que *password2* champ type, qui est chiffré avec KMF. Les mots de passe utilisateur, qui sont utilisés pour vérifier les demandes de point de terminaison entrantes, sont stockés en tant que valeur de hachage dans la table Utilisateur dans un *password* champ type (SHA 256). Pour plus d'informations sur ce chiffrement, consultez Chiffrement Password2 avec KMF

Configurer OAuth

Configurez et activez OAuth, activez la propriété système OAuth, créez un point de terminaison d'application OAuth pour permettre aux applications clientes externes d'accéder à l'instance et définissez les paramètres OAuth.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Assurez-vous que le module d'extension OAuth est actif et que la propriété d'activation OAuth est définie sur vrai.
2. Créez un registre d'application OAuth en utilisant l'une des méthodes suivantes :
   - Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement **d'application cliente OAuth** et génère un ID client et un secret client dont le client a besoin pour accéder aux ressources restreintes sur l'instance.
   - Utilisez un fournisseur OAuth tiers qui fournit l'autorisation d'accès à votre instance.

     Spécifiez un profil OAuth et un périmètre OAuth lorsque vous vous connectez à un autre fournisseur OAuth.
3. Configurez vos applications clientes pour créer un HTTP POST qui demande un jeton OAuth. L'application doit également être en mesure d'analyser la réponse JSON pour utiliser le jeton d'accès et le jeton d'actualisation renvoyés.

Activer OAuth

Par défaut, le module **d'extension OAuth 2.0 (com.snc.platform.security.oauth)** est actif sur les instances nouvelles et mises à niveau. Si le module d'extension n'est pas actif sur votre instance, vous pouvez l'activer.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Définir la propriété OAuth

Pour générer des jetons OAuth 2.0 vers des applications enregistrées, la propriété `com.snc.platform.security.oauth.is.active` doit être active pour l'instance.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour utiliser OAuth 2.0, saisissez **sys_properties.list** dans le navigateur et sélectionnez **Nouveau**. Vous pouvez également ouvrir la liste des propriétés système en accédant à **Tous** > **Propriétés système** > **Toutes les propriétés** > .
2. Remplissez le formulaire avec les paramètres suivants :
   - **Nom** : com.snc.platform.security.oauth.is.active
   - **Type** : vrai | faux
   - **Valeur** : vrai

Modifier le paramètre du mot de passe OAuth

Utilisez cette propriété pour vous assurer que seuls les paramètres du corps POST sont acceptés comme entrée pour tous les types d'accord pris en charge.

L'envoi d'informations sensibles sur les paramètres de requête URI peut entraîner la divulgation d'informations sensibles par les clients, le serveur ou tout hôte entre les demandes. À partir de la version Madrid, cette nouvelle propriété garantit que seuls les paramètres de corps POST sont acceptés comme entrée pour tous les types d'accord pris en charge. Les types d'octroi pris en charge sont les suivants :

- Code d'autorisation
- mot de passe
- Informations d'identification du client
- Actualiser le jeton

Propriété du paramètre de mot de passe OAuth

Propriété	Description
glide.oauth.allow.parameters.in.post.body.only	Cette propriété est définie sur vrai pour zBoots uniquement, dans le cadre du module d'extension OAuth 2.0. Si vous avez besoin de ce paramètre pour votre instance, créez et définissez la propriété sur vrai.

Entrant OAuth

L'authentification entrante OAuth permet aux applications externes de confiance d'accéder en toute sécurité aux API ServiceNow, garantissant ainsi des connexions contrôlées et autorisées.

Vous devez disposer de l'un des rôles suivants pour configurer ou gérer les intégrations OAuth dans le système :

- oauth_admin
- mi_admin
- admin

L'authentification entrante permet aux applications externes telles que des systèmes tiers ou d'autres ServiceNow® instances de se connecter en toute sécurité aux ServiceNow API. L'authentification entrante confirme que seuls les clients de confiance peuvent accéder à votre instance ServiceNow de manière contrôlée et sécurisée. ServiceNow prend en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plusieurs types d'autorisations OAuth 2.0, chacun conçu pour des scénarios d'intégration spécifiques. Utilisez les informations suivantes pour choisir le type d'accord qui correspond le mieux à votre cas d'utilisation :

Octroi du code d'autorisation

Scénario d'utilisation idéal	Fonction
Applications qui doivent accéder aux données utilisateur pour le compte de l'utilisateur avec le consentement de l'utilisateur. Exemple : applications Web, mobiles ou de bureau agissant pour le compte d'un utilisateur.	L'utilisateur lance le processus de connexion à partir de l'application cliente, qui le redirige vers une ServiceNow page de connexion. Une fois que l'utilisateur s'est connecté et a donné son consentement, l'application cliente reçoit un code d'autorisation. L'application cliente échange le code d'autorisation avec l'instance ServiceNow contre un jeton d'accès. L'octroi de code d'autorisation est le workflow le plus sécurisé et le plus utilisé pour les intégrations orientées utilisateur. Il prend en charge à la fois les clients confidentiels (avec un secret client) et les clients publics utilisant Proof Key for Code Exchange (PKCE).

Pour plus d'informations sur le workflow et la configuration d'octroi du code d'autorisation, voir Attribution du code d'autorisation

Octroi des informations d'identification du client

Scénario d'utilisation idéal	Fonction
Les applications clientes telles que les services back-end ou les intégrations de systèmes automatisées qui doivent accéder aux ServiceNow API sans implication de l'utilisateur.	L'application cliente s'authentifie directement auprès de l'instance à l'aide ServiceNow de ses propres informations d'identification (ID client et clé secrète). Une fois authentifiée, l'application reçoit un jeton d'accès ServiceNow pour accéder aux API.

Pour plus d'informations sur le workflow et la configuration d'octroi des informations d'identification du client, reportez-vous à la section Attribution des informations d'identification du client.

Flux de jetons d'ID tiers

Scénario d'utilisation idéal	Fonction
Scénarios d'authentification fédérée où ServiceNow les trusts, l'identité ou les jetons d'accès émis par des fournisseurs d'identité externes tels que Azure AD ou Okta.	L'application cliente obtient un ID ou un jeton d'accès auprès d'un fournisseur d'identité tiers de confiance et l'inclut dans l'en-tête d'autorisation lors des demandes d'API à l'instance ServiceNow . ServiceNow valide le jeton et, si elle est approuvée, accorde l'accès en fonction de l'identité qu'elle affirme. Cela permet une authentification unique (SSO) transparente et une authentification fédérée entre les systèmes.

Pour plus d'informations sur le flux et la configuration des jetons tiers, consultezOctroi de jeton tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bourse JWT Bearer

Scénario d'utilisation idéal	Fonction
Applications clientes qui ont besoin d'un accès sécurisé aux ServiceNow ressources, soit pour le compte d'un utilisateur, soit en tant que lui-même, sans nécessiter d'interaction de l'utilisateur ni stocker de secret partagé. L'application cliente crée un jeton Web JSON signé (JWT) qui inclut les revendications liées à l'identité, telles que l'utilisateur ou le système qu'elle représente. Il le présente ensuite à l'instance ServiceNow pour demander un jeton d'accès.	**Lorsque vous agissez au nom d'un utilisateur :** Le jeton représente un utilisateur précédemment authentifié. Cela permet un accès sécurisé et transparent sans avoir à demander à nouveau à l'utilisateur des informations d'identification ou son consentement. Le jeton signé affirme l'identité de l'utilisateur, ce qui permet ServiceNow de faire confiance à la demande sans nécessiter d'interaction en temps réel de l'utilisateur. **Lorsqu'il agit en son propre nom :** Le jeton identifie et authentifie directement l'application cliente. Au lieu d'utiliser un secret partagé, le client signe le jeton avec une clé privée, ce qui en fait une alternative plus sûre à l'octroi d'informations d'identification du client.

Pour plus d'informations sur le workflow et la configuration de la subvention JWT Bearer, reportez-vous à la section Octroi de porteur de jeton Web JSON.

Attribution des informations d'identification du mot de passe de propriétaire de ressource

Scénario d'utilisation idéal	Fonction
Applications clientes internes hautement fiables dans des environnements contrôlés où l'application collecte directement les informations d'identification de l'utilisateur.	L'application cliente collecte le nom d'utilisateur et le mot de passe de l'utilisateur et le redirige vers l'instance pour obtenir un jeton d'accès ServiceNow . Le workflow contourne les écrans de redirection et de consentement, mais expose les informations d'identification de l'utilisateur à l'application cliente. ServiceNow vous recommande d'implémenter les informations d'identification du mot de passe de propriétaire de ressource uniquement dans des environnements hérités ou contrôlés.

Pour plus d'informations sur le workflow et la configuration d'octroi des informations d'identification de mot de passe de propriétaire de ressource, reportez-vous à la section Attribution des informations d'identification du mot de passe de propriétaire de ressource.

Subventions implicites

Scénario d'utilisation idéal	Fonction
Applications monopages (SPA) héritées ou applications basées sur un navigateur qui ne peuvent pas stocker en toute sécurité un secret client et nécessitent un flux d'authentification côté client léger.	L'utilisateur se connecte via un navigateur. L'application cliente reçoit le jeton d'accès directement dans l'URL après la connexion, en ignorant l'étape du code d'autorisation intermédiaire. Ce flux a été conçu à l'origine pour les clients publics qui s'exécutent entièrement dans le navigateur, où il n'est pas possible de stocker des secrets en toute

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scénario d'utilisation idéal	Fonction
	sécurité. Bien qu'il simplifie la mise en œuvre, il expose les jetons dans le navigateur, ce qui augmente le risque d'interception. Pour renforcer la sécurité, ServiceNow recommande d'implémenter l'octroi d'un code d'autorisation avec PKCE.

Pour plus d'informations sur le workflow et la configuration de l'octroi implicite, reportez-vous à la section Attributions implicites OAuth.

Périmètres OAuth

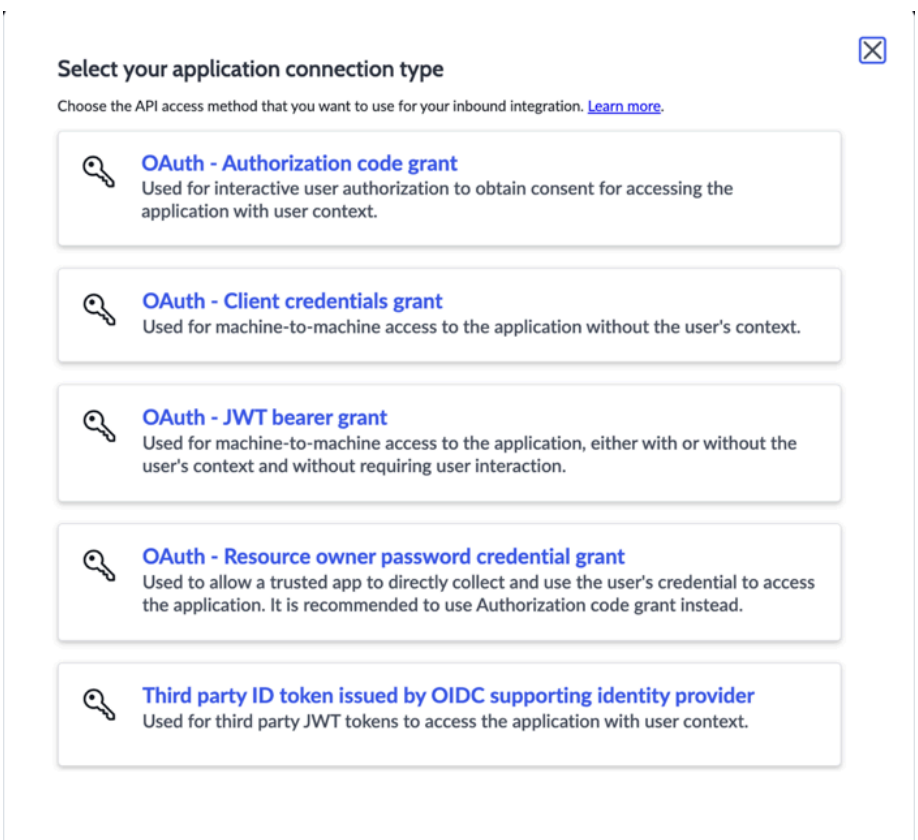
Vous pouvez définir la prise en charge du périmètre d'authentification OAuth pour l'API REST. Le périmètre OAuth permet d'accéder uniquement aux API REST particulières. Pour plus d'informations, consultez Périmètre d'authentification REST API.

Nouvelle expérience d'intégrations entrantes

Le nouveau workflow d'intégration entrante dans la console d'identité ServiceNow machine offre une expérience améliorée pour la gestion des intégrations entrantes.

Méthodes d'intégrations entrantes

Sur l'instance, accédez à **Tous** > **Console des identités des machines** > **Intégrations entrantes** > **Nouvelle intégration**. Choisissez le type de connexion d'application (type d'octroi).



Pour en savoir plus sur les différents types d'attribution et leur configuration, consultez les rubriques suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Attribution du code d'autorisation
- Attribution des informations d'identification du client
- Octroi de porteur de jeton Web JSON
- Attribution des informations d’identification du mot de passe de propriétaire de ressource
- Octroi de jeton tiers

Attribution du code d'autorisation

L’attribution du code d’autorisation OAuth est un flux sécurisé et largement utilisé pour les applications Web, mobiles ou de bureau qui accèdent aux données utilisateur avec son consentement. Il prend en charge à la fois les clients privés (à l’aide d’un secret client) et les clients publics (à l’aide de PKCE).

Dans le flux d’octroi du code d’autorisation, ServiceNow fonctionne à la fois comme serveur d’autorisation (gérant l’authentification utilisateur et l’émission de jeton) et serveur de ressources (hébergeant les API). Si la SSO est activée, ServiceNow redirige l’utilisateur vers le fournisseur d’identité (IdP) configuré pour authentification. Une fois l’utilisateur authentifié avec succès, le contrôle revient à ServiceNow, qui émet alors le code d’autorisation. Ce processus garantit que, même avec authentification externe, ServiceNow l’autorité reste l’autorité pour l’émission des jetons et la gestion de l’accès aux API.

Remarque :
Si vous souhaitez utiliser votre propre fournisseur d’identité (tel que Azure AD ou Okta) comme serveur d’autorisation, envisagez d’utiliser le Octroi de jeton tiers flux.

Information associée

Workflow d’octroi de code d’autorisation

Configurer un octroi de code d’autorisation OAuth

Workflow d’octroi de code d’autorisation

L’attribution du code d’autorisation OAuth est un flux sécurisé et largement utilisé pour les applications Web, mobiles ou de bureau qui accèdent aux données utilisateur avec son consentement. Il prend en charge à la fois les clients privés (à l’aide d’un secret client) et les clients publics (à l’aide de PKCE).

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

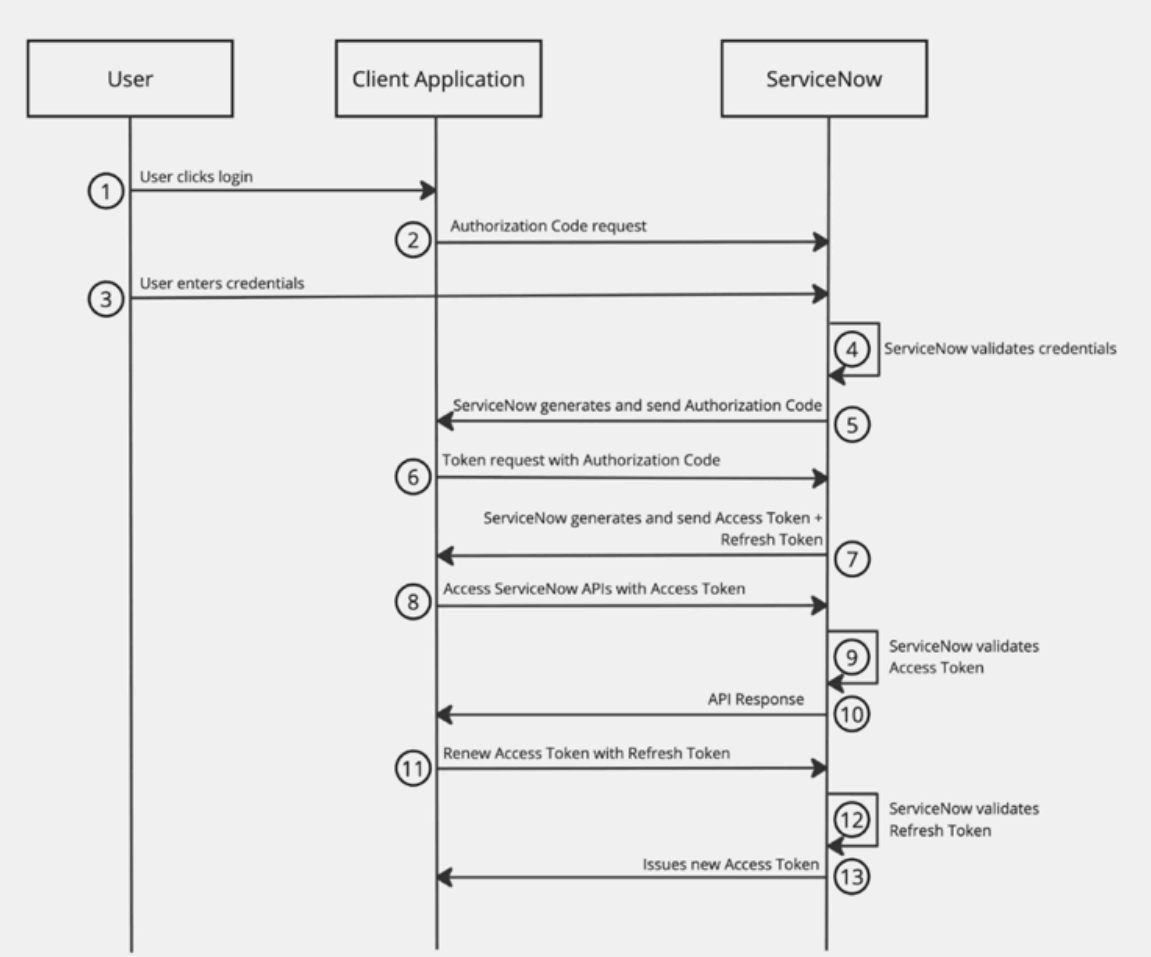
Pourquoi et quand exécuter cette tâche

Cette collection de rubriques fournit des informations sur la façon dont une application cliente peut utiliser le flux d’octroi du code d’autorisation pour obtenir un jeton de ServiceNow et effectuer des appels d’API avec ce jeton. Les clients privés utilisent le secret client, tandis que les clients publics utilisent le défi de code PKCE.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow d'autorisation



Procédure

1. Connectez-vous à partir de l'application cliente.

   L'utilisateur commence le processus de connexion à partir de l'interface de l'application cliente.

2. Lancez la demande d'autorisation.

   Le client redirige l'utilisateur vers le point de terminaison d'autorisation ServiceNow. La méthode d'initiation de la demande d'autorisation dépend du type de client : public ou privé.

   Clients publics

   Les clients publics (exemple : applications mobiles ou à page unique) ne peuvent pas stocker un secret client en toute sécurité. Par conséquent, ils doivent utiliser **la clé de preuve pour l'échange de code (PKCE)** pour renforcer la sécurité.

   - Dans la demande d'autorisation, incluez la **contestation de code PKCE** et spécifiez la **méthode de contestation de code**.
   - Pendant la demande de jeton, le client doit envoyer le **vérificateur de code** pour valider le code d'autorisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Effectuez une demande GET au point de terminaison d'autorisation avec les paramètres suivants :

```
Method: GET
Endpoint: https://<servicenow_base_url>/oauth_auth.do
```

Paramètres de demande d'autorisation (Client public : PKCE)

Paramètre	Obligatoire	Description
response_type	Oui	Définissez la valeur sur code pour lancer le flux de code d'autorisation.
client_id	Oui	L'identificateur unique pour votre application cliente. Format : YOUR_CLIENT_ID
redirect_uri	Oui	L'URI auquel ServiceNow envoie le code d'autorisation. Exemple : https://yourapp.com/callback
code_challenge	Oui	Hachage SHA-256 encodé en base64url du vérificateur de code. Ceci est utilisé dans le cadre du flux PKCE.
code_challenge_method	Oui	Spécifie la méthode de transformation utilisée pour le test de code. Réglez sur S256.
périmètre	Facultatif	Une liste de champs d'application demandés séparés par des espaces. Exemple : incident_read incident_write.
État	Oui	Une valeur générée par le client utilisée pour éviter les attaques CSRF. La valeur est renvoyée inchangée dans l'URI de redirection, ce qui permet au client de la valider.

Remarque :
À partir de la version Madrid, la propriété système glide.oauth.state.parameter.required rend obligatoire l'utilisation du paramètre state dans les demandes OAuth. La propriété d'état est définie sur vrai par défaut dans les nouvelles instances et est facultative dans les instances mises à niveau. En cas de paramètre d'état manquant, la demande d'autorisation échoue et l'erreur suivante s'affiche : Paramètre d'état manquant dans la demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clients privés

Les clients privés (exemple : applications côté serveur) peuvent stocker un secret client en toute sécurité et n'ont pas besoin de PKCE.

- La demande d'autorisation est lancée en redirigeant l'utilisateur vers le point de terminaison d'autorisation. **Aucune contestation du secret client ou du code PKCE n'est requise** dans cette étape.
- Au cours de la demande de jeton, le client inclut le **secret client** ainsi que le **code d'autorisation** pour obtenir le jeton d'accès.

Effectuez une demande GET au point de terminaison d'autorisation avec les paramètres suivants :

```
Method: GET
Endpoint: https://<servicenow_base_url>/oauth_auth.do
```

Paramètres de demande d'autorisation (secret du client privé)

Paramètre	Obligatoire	Description
response_type	Oui	Définissez la valeur sur code pour lancer le flux de code d'autorisation.
client_id	Oui	L'identificateur unique pour votre application cliente. Format : YOUR_CLIENT_ID
redirect_uri	Oui	L'URI auquel ServiceNow envoie le code d'autorisation. Exemple : https://yourapp.com/callback
périmètre	Facultatif	Une liste de champs d'application demandés séparés par des espaces. Exemple : incident_read incident_write.
État	Oui	Valeur générée par le client et utilisée pour éviter les attaques de contrefaçon de requête intersite (CSRF). La valeur est renvoyée inchangée dans l'URI de redirection, ce qui permet au client de la valider.

3. Connectez-vous et donnez votre consentement d'accès à l'application cliente.
   Connectez-vous ServiceNow (ou IdP, si SSO est activé) et donnez votre consentement d'accès à l'application cliente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. ServiceNow (ou IdP, si SSO est activé) valide les informations d'identification et ServiceNow renvoie un code d'autorisation au client.

   Une fois l'authentification réussie, le navigateur est redirigé vers le `redirect_uri` et le code d'autorisation est inclus dans la chaîne de requête :

   ```
   https://yourapp.com/callback?code=AUTH_CODE&state=xyz123
   ```

5. Lancez la demande d'autorisation.

   Le client redirige l'utilisateur vers le point de terminaison d'autorisation ServiceNow pour un jeton d'accès. La méthode d'initiation de la demande d'autorisation dépend du type de client : public ou privé.

   Clients publics

   Les clients publics (exemple : applications mobiles ou à page unique) ne peuvent pas stocker un secret client en toute sécurité. Par conséquent, ils doivent utiliser **la clé de preuve pour l'échange de code (PKCE)** pour renforcer la sécurité.

   - Dans la demande d'autorisation, incluez la **contestation de code PKCE** et spécifiez la **méthode de contestation de code**.
   - Pendant la demande de jeton, le client doit envoyer le **vérificateur de code** pour valider le code d'autorisation.

   Le client envoie une demande POST au point de terminaison de jeton avec les paramètres suivants :

   ```
   Method: POST
   Endpoint: https://<servicenow_base_url>/oauth_token.do
   Headers: Content-Type: application/x-www-form-urlencoded
   ```

   Paramètres de demande de jeton (Client public-PKCE)

Paramètre	Obligatoire	Description
`grant_type`	Oui	Définissez la valeur sur `authorization_code` pour échanger le code contre un jeton.
`code`	Oui	Le code d'autorisation reçu du point de terminaison d'autorisation.
`redirect_uri`	Oui	L'URI utilisé dans la demande d'autorisation initiale. Exemple : https://yourapp.com/callback
`client_id`	Oui	L'identificateur unique pour votre application cliente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Obligatoire	Description
code_verifier	Oui	Chaîne d'origine utilisée pour générer le code_challenge PKCE.
État	Oui	Une valeur générée par le client utilisée pour aider à prévenir les attaques CSRF. La valeur est renvoyée inchangée dans l'URI de redirection, ce qui permet au client de la valider.

Clients privés

Les clients privés (exemple : applications côté serveur) peuvent stocker un secret client en toute sécurité et n'ont pas besoin de PKCE.

- La demande d'autorisation est lancée en redirigeant l'utilisateur vers le point de terminaison d'autorisation. **Aucune contestation du secret client ou du code PKCE n'est requise** dans cette étape.
- Au cours de la demande de jeton, le client inclut le **secret client** ainsi que le **code d'autorisation** pour obtenir le jeton d'accès.

Effectuez une demande POST au point de terminaison d'autorisation avec les paramètres suivants :

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Paramètres de demande de jeton (client privé : secret client)

Paramètre	Obligatoire	Description
grant_type	Oui	Définissez la valeur sur authorization_code pour échanger le code contre un jeton.
code	Oui	Le code d'autorisation reçu du point de terminaison d'autorisation.
redirect_uri	Oui	L'URI utilisé dans la demande d'autorisation initiale. Exemple : https://yourapp.com/callback
client_id	Oui	L'identificateur unique pour votre application cliente.
client_secret	Oui	Clé secrète du client utilisée pour s'authentifier avec le point de terminaison de jeton.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Obligatoire	Description
État	Oui	Une valeur générée par le client utilisée pour aider à prévenir les attaques CSRF. La valeur est renvoyée inchangée dans l'URI de redirection, ce qui permet au client de la valider.

6. Accéder aux API avec le jeton d'accès ServiceNow .

   Exemple :

   Effectuez une demande GET auprès des API à l'aide du jeton d'accès. Incluez le jeton d'accès dans l'en-tête d'autorisation .

```
Method: GET
End Point: https://<servicenow_base_url>/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

7. Renouvelez le jeton d'accès s'il a expiré.
   Effectuez une demande POST pour actualiser le jeton d'accès (clients privés uniquement) avec les paramètres suivants :

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Paramètres de demande de jeton d'actualisation (client privé)

Paramètre	Obligatoire	Description
grant_type	Oui	Définissez la valeur sur refresh_token pour demander un nouveau jeton d'accès.
refresh_token	Oui	Le jeton d'actualisation précédemment émis par le point de terminaison de jeton.
client_id	Oui	L'identificateur unique pour votre application cliente.
client_secret	Oui	Clé secrète du client utilisée pour s'authentifier avec le point de terminaison de jeton.

Configurer un octroi de code d'autorisation OAuth

Configurez l'octroi du code d'autorisation OAuth pour activer une authentification utilisateur sécurisée et interactive afin de permettre aux applications d'accéder aux ressources au nom des utilisateurs. L'attribution du code d'autorisation OAuth vérifie que l'accès à l'API est accordé en fonction de l'identité et des autorisations de l'utilisateur.

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Console des identités des machines** > **Intégrations entrantes** > **Nouvelle intégration** > > **Octroi du code d'autorisation OAuth**.
   La page Nouvel enregistrement s'affiche.
2. Mettez à jour les champs de texte du formulaire Détails avec les informations appropriées.

Formulaire Détails

Champ	Description
Nom de l'entité OAuth	Nom de l'entité OAuth.
URL de redirection	URL vers laquelle le code d'autorisation doit être envoyé après authentification.
ID client	ID unique affecté pour identifier l'application.
Secret client	Clé secrète que seules l'application et le serveur d'autorisation peuvent identifier. L'application utilise cette clé pour s'authentifier et obtenir des jetons d'accès.

Cochez la **case Ceci est un client public** si l'application ne peut pas stocker les informations d'identification en toute sécurité et ne nécessite pas de clé secrète pour prouver son identité pendant l'autorisation. Les informations secrètes du client sont traitées pour les clients publics.

3. Mettez à jour les champs de texte du formulaire Options avancées (facultatif) avec les informations appropriées.

Formulaire Options avancées

Champ	Description
Durée de vie du jeton d'accès	Durée (en secondes) pendant laquelle le jeton d'accès OAuth reste valide avant son expiration. **Remarque :** La valeur par défaut est de 1 800 secondes.
Durée de vie du jeton d'actualisation	Durée (en secondes) pendant laquelle le jeton d'actualisation OAuth reste valide avant son expiration. **Remarque :** La valeur par défaut est de 8 640 000 secondes.
URL de connexion	Point de terminaison de redirection HTTP à authentifier auprès du serveur d'autorisation.
URL du logo	Adresse Web d'une image qui représente l'application pendant le processus d'authentification et d'autorisation. Il s'affiche sur l'écran de consentement du serveur d'autorisation pour vous aider à reconnaître l'application demandeuse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'application de la restriction de jeton applique des limitations sur la façon dont un jeton d'accès OAuth peut être utilisé, améliorant la sécurité en vérifiant que les jetons ne sont valides que dans des conditions spécifiques. Cochez la case **Appliquer la restriction de jeton** pour limiter les jetons d'accès OAuth à des API spécifiques définies dans la politique d'accès API. Si la restriction Appliquer le jeton est désactivée, le jeton peut être utilisé dans d'autres API REST.

4. Mettez à jour les champs de texte du formulaire **(facultatif) du périmètre d'authentification** avec les informations appropriées. Le périmètre d'authentification définit le niveau d'accès d'une application à une ressource. Sélectionnez le périmètre d'authentification pour les API REST spécifiques auxquelles vous souhaitez accéder.

Formulaire du périmètre d'authentification

Champ	Description
Périmètre d'authentification	Niveau d'accès qu'une application a à une ressource. Le périmètre d'authentification limite les actions qu'un jeton d'accès peut effectuer sur les API ou les données.
Autorisation de limite	Noms des API pour lesquelles vous souhaitez restreindre l'autorisation.

5. Sélectionnez **Créer un nouveau périmètre d'authentification** pour ajouter un nouveau périmètre d'authentification.
6. Sélectionnez **Enregistrer**.
   Un nouvel octroi de code d'autorisation OAuth est créé.
7. Accéder à **Tous** > **Intégrations entrantes** > **Registres d'application** pour afficher l'octroi du code d'autorisation OAuth nouvellement créé.

Attribution des informations d'identification du client

Utilisez le type d'accord Informations d'identification du client OAuth pour les services back-end ou les intégrations automatisées qui accèdent aux ServiceNow® API sans interaction de l'utilisateur. L'application cliente s'authentifie directement à l'aide de son ID client et de son secret, et reçoit un jeton d'accès qui représente l'application elle-même, et non l'utilisateur.

Information associée

Workflow d'octroi des informations d'identification du client

Configurer une autorisation d'informations d'identification client OAuth

Workflow d'octroi des informations d'identification du client

Authentifiez une application cliente à l'aide d'un workflow d'informations d'identification client. Le workflow d'attribution des informations d'identification du client est utilisé par les services back-end ou les intégrations système pour accéder ServiceNow® aux API sans intervention de l'utilisateur.

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Pourquoi et quand exécuter cette tâche

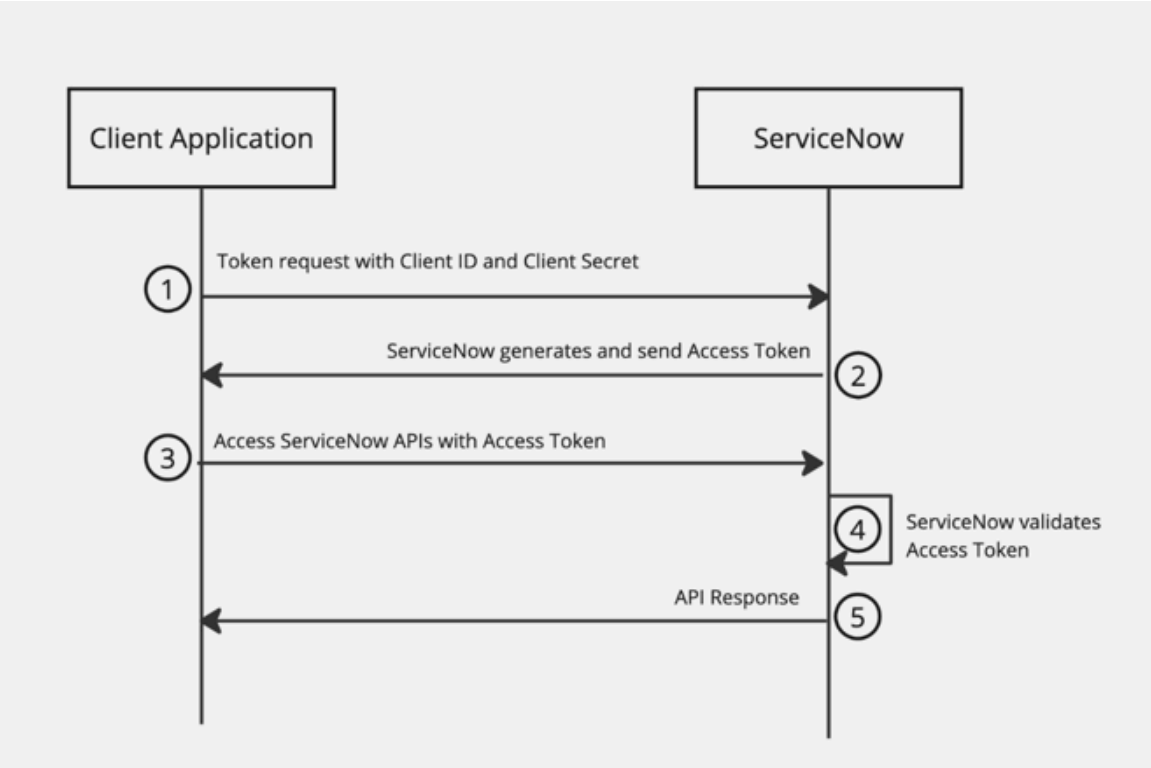
Ce workflow décrit comment une application cliente (service back-end ou intégration système) s'authentifie directement à ServiceNow l'aide des informations d'identification de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

son client sans interaction de l'utilisateur. L'application demande un jeton d'accès à l'aide de son ID client et de son secret client, qui ServiceNow valident avant d'émettre le jeton. Le client utilise ensuite ce jeton pour accéder ServiceNow aux API. ServiceNow valide chaque demande avant de renvoyer la réponse appropriée.

Workflow d'octroi des informations d'identification du client



Procédure

1. **L'application cliente envoie une demande de jeton** au point de terminaison ServiceNow avec les paramètres suivants :

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
```

Paramètres de demande de jeton

Paramètre	Obligatoire	Description
grant_type	Oui	Type d'accord OAuth 2.0. Exemple : client_credentials
client_id	Oui	Identificateur unique pour l'application cliente. Exemple : YOUR_CLIENT_ID
client_secret	Oui	Secret associé à l'ID client. Exemple :YOUR_CLIENT_SECRET
scope	Facultatif	Autorisations demandées pour le jeton d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Obligatoire	Description
		Exemple : incident_read incident_write

2. ServiceNow Valide les informations d'identification et renvoie le jeton d'accès.
3. Effectuez une demande d'API avec le jeton d'accès.

   Incluez le jeton d'accès dans l'en-tête d'autorisation de chaque demande d'API.

```
Method: POST
Endpoint: https://<servicenow_base_url>/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

4. ServiceNow valide le jeton et renvoie la réponse API appropriée.

> **Remarque :**
> Utilisez le workflow d'attribution d'informations d'identification client uniquement avec des applications côté serveur approuvées. Maintenez le client_secret en toute sécurité. Assurez-vous de ne pas utiliser le client_secret dans des environnements côté client tels que des navigateurs ou des applications mobiles.

Configurer une autorisation d'informations d'identification client OAuth

Configurez l'accord d'informations d'identification du client OAuth pour une authentification sécurisée de machine à machine sans interaction de l'utilisateur. Il authentifie les applications à l'aide des informations d'identification du client et accorde un accès contrôlé à l'API avec des autorisations incluses dans le périmètre.

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Procédure

1. Accédez à la **Console des identités des machines** > > **Intégrations entrantes** > > **Nouvelle intégration** > **Octroi des informations d'identification du client OAuth**.
   La page de configuration des informations d'identification du client OAuth s'affiche.
2. Mettez à jour les champs de texte du formulaire Détails avec les informations appropriées.

Formulaire Détails

Champ	Description
Nom	Nom de l'entité OAuth.
Utilisateur de l'application OAuth	Nom d'utilisateur du compte de service qu'une application authentifie et autorise via OAuth.
ID client	ID unique affecté pour identifier l'application.
Secret client	Clé secrète que seules l'application et le serveur d'autorisation peuvent identifier. L'application utilise cette clé pour s'authentifier et obtenir des jetons d'accès.

Sélectionnez la case à cocher **Activé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Mettez à jour les champs de texte du formulaire Options avancées (facultatif) avec les informations appropriées.
4. Mettez à jour les champs de texte du formulaire **(facultatif) du périmètre d'authentification** avec les informations appropriées.
   Le périmètre d'authentification définit le niveau d'accès d'une application à une ressource. Sélectionnez le périmètre d'authentification pour les API REST spécifiques auxquelles vous souhaitez accéder.

Formulaire du périmètre d'authentification

Champ	Description
Périmètre d'authentification	Niveau d'accès qu'une application a à une ressource. Le périmètre d'authentification limite les actions qu'un jeton d'accès peut effectuer sur les API ou les données.
Autorisation de limite	Noms des API pour lesquelles vous souhaitez restreindre l'autorisation.

   a. Sélectionnez **Créer un nouveau périmètre d'authentification** pour ajouter un nouveau périmètre d'authentification.
5. Sélectionnez **Enregistrer**.
   Un nouvel accord d'informations d'identification client OAuth est créé.
6. Accéder à **Tous** > **Intégrations entrantes** > **Registres d'application** pour afficher l'octroi d'informations d'identification du client nouvellement créé.

Octroi de jeton tiers

L'attribution de jeton tiers permet ServiceNow® d'accepter des jetons d'identité provenant de fournisseurs d'identité externes de confiance, tels qu'Azure AD ou Okta. L'attribution de jetons tiers fournit un accès sécurisé basé sur les jetons. Cette méthode prend en charge l'accès sécurisé et l'authentification unique (SSO) dans les scénarios d'authentification fédérée.

L'application cliente demande un ID ou un jeton d'accès auprès d'un fournisseur d'identité externe de confiance, tel qu'Azure AD ou Okta, et l'inclut dans l'en-tête d'autorisation des demandes d'API vers ServiceNow®. ServiceNow® valide le jeton et, si elle est approuvée, accorde l'accès en fonction de l'identité déclarée.

Vous pouvez utiliser les comptes d'un fournisseur d'identité tiers pour accéder à l'API ServiceNow® pour :

- Workflow de jeton tiers pour les comptes d'utilisateurs
- Workflow de jeton tiers pour les comptes de services

Workflow de jeton tiers pour les comptes d'utilisateurs

Ce workflow est basé sur le concept de fédération de jetons. Elle permet aux applications clientes d'obtenir des jetons directement auprès d'un IdP et de les utiliser pour accéder ServiceNow aux API.

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Traduction automatique

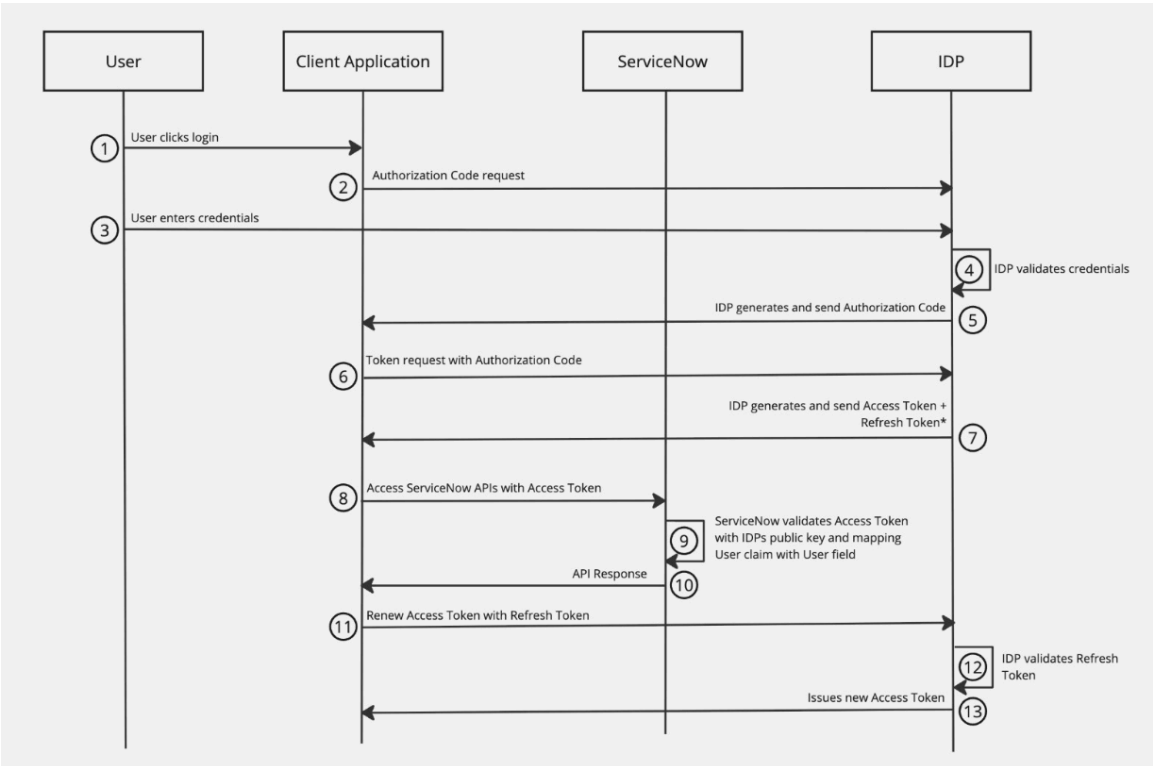
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'application cliente tierce demande des jetons directement auprès de votre fournisseur d'identité (IdP). La méthode d'authentification entre le client et l'IdP est flexible et peut être configurée pour répondre à vos besoins spécifiques. Une fois l'authentification réussie, l'IdP émet un jeton d'ID ou un jeton d'accès et, éventuellement, un jeton de rafraîchissement. Ces jetons sont envoyés directement à l'application cliente, qui les utilise ensuite pour accéder ServiceNow aux API.

Remarque :
ServiceNow valide le jeton à l'aide de la clé publique configurée lors de la configuration et accorde l'accès aux API demandées. Assurez-vous que le jeton est au format JSON Web Token (JWT).

Workflow de compte utilisateur



Remarque :
Ce diagramme est fourni à titre d'illustration. Il affiche le flux d'octroi du code d'autorisation entre votre application cliente et le fournisseur d'identité. Le flux de travail est flexible. Vous pouvez utiliser un flux différent en fonction de vos besoins.

Procédure

1. Configurez votre application client tierce.

   Configurez votre application cliente tierce pour demander des jetons directement auprès de votre fournisseur d'identité (IdP). Sélectionnez la méthode d'authentification qui correspond le mieux à vos besoins de sécurité et d'intégration.

2. Créez un client OAuth dans ServiceNow.

   Fournissez les détails requis pour activer la validation des jetons entrants de votre fournisseur d'identité (IdP). Pour en savoir plus sur la configuration, consultez Configurer un jeton d'ID de tiers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow de jeton tiers pour les comptes de services

Suivez les étapes de création d'un workflow de jeton tiers pour les comptes d'utilisateurs. En outre, créez un compte sys_user correspondant dans ServiceNow pour votre compte de service. Contrairement aux utilisateurs humains qui ont généralement des enregistrements existants dans ServiceNow, les comptes de service sont spécifiques à l'application et nécessitent une création manuelle pour établir une identité valide dans la plateforme.

Avant de commencer

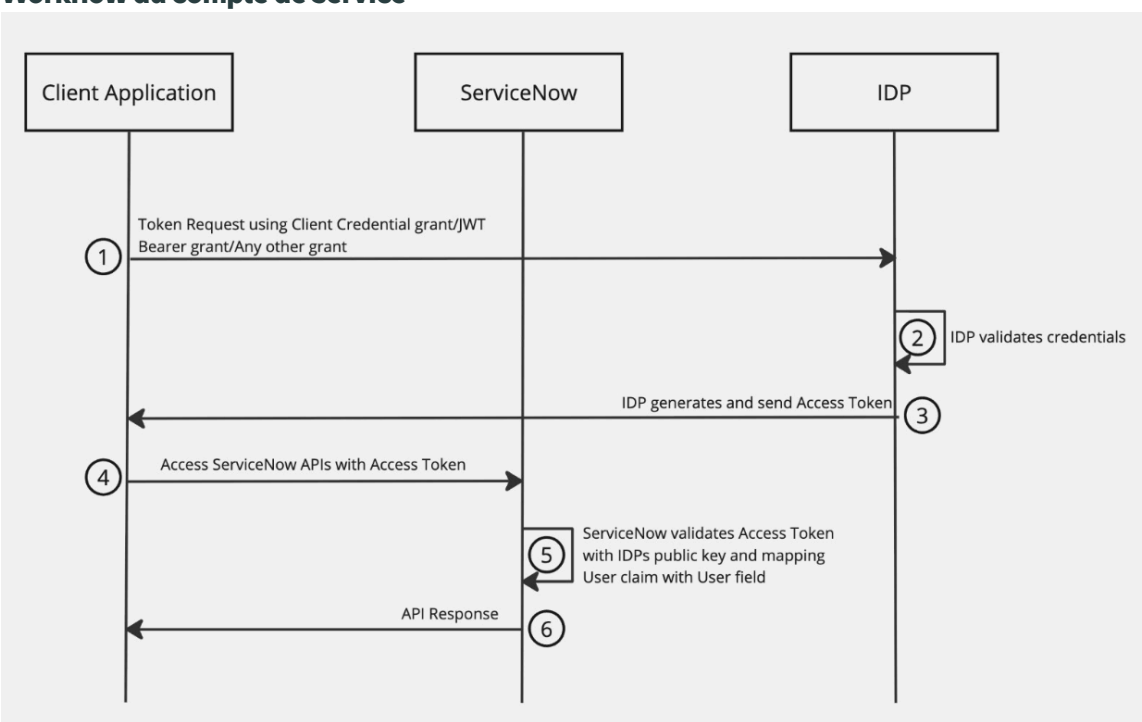
Rôle requis : oauth_admin, mi_admin, admin

Pourquoi et quand exécuter cette tâche

Lorsqu'une application tierce s'authentifie à l'aide d'un jeton provenant d'un fournisseur d'identité externe (IdP), elle ServiceNow a besoin d'un enregistrement utilisateur correspondant pour mapper l'identité et appliquer des contrôles d'accès.

La valeur de la réclamation configurée lors de la configuration initiale dans le jeton émis par votre fournisseur d'identités est mappée au champ utilisateur spécifié lors de cette configuration. Ce compte représente l'identité de service dans ServiceNow. Vous pouvez restreindre ce compte à l'accès à l'API uniquement et affecter les autorisations nécessaires en ajoutant les rôles et les groupes appropriés.

Workflow du compte de service



Procédure

1. Suivez les étapes indiquées dans la configuration du flux de jetons d'ID du compte d'utilisateur.
2. Créez un compte sys-user pour ServiceNow représenter l'identité de votre compte de service. Assurez-vous que la valeur de réclamation de jeton correspond à celle de la valeur du champ utilisateur mappé (telle que user_name ou e-mail) de l'enregistrement utilisateur. Exemple : user_name, e-mail.
   a. Sélectionnez l'option Accès au service Web uniquement pour restreindre le compte à l'accès à l'API.
   b. Affectez les rôles et les groupes requis pour accorder l'autorisation appropriée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La ServiceNow plateforme mappe la déclaration configurée au champ d'utilisateur spécifié dans l'enregistrement de sys_user . Il applique l'accès en fonction des rôles et des groupes affectés à cet utilisateur.

3. Effectuez une demande GET avec l'en-tête d'autorisation vers le point de terminaison suivant :

```
Method: GET
Endpoint: https:// <servicenow_base_url> /api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

Configurer un jeton d'ID de tiers

Configurez un jeton d'ID tiers pour activer l'authentification sécurisée en vérifiant les identités des utilisateurs via un fournisseur d'identités externe. Le jeton d'ID tiers améliore la sécurité en réduisant les informations d'identification stockées, confirme une authentification transparente et prend en charge l'interopérabilité avec les normes du secteur telles qu'OpenID Connect (OIDC).

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Procédure

1. Accédez à la **Console des identités des machines** > > **Intégrations entrantes** > **Nouvelle intégration** > **Jeton d'ID tiers**.
2. Mettez à jour les champs de texte du formulaire **Détails** avec les informations appropriées.

Formulaire Détails

Champ	Description
Nom	Nom fourni par le propriétaire de ressource (utilisateur) lors de l'authentification.
ID client	ID unique affecté pour identifier l'application.
Secret client	Clé secrète que seules l'application et le serveur d'autorisation peuvent identifier. L'application utilise cette clé pour s'authentifier et obtenir des jetons d'accès.

L'application de la restriction de jeton applique des limitations sur la façon dont un jeton d'accès OAuth peut être utilisé, renforçant la sécurité en vérifiant que les jetons ne sont valides que dans des conditions spécifiques. Cochez la case **Appliquer la restriction de jeton** pour limiter les jetons d'accès OAuth à des API spécifiques définies dans la politique d'accès API. Si **Appliquer la restriction de jeton** est désactivé, le jeton peut être utilisé dans d'autres API REST.

3. Mettez à jour les champs de texte du formulaire **Options avancées (facultatif)** avec les informations appropriées.

Formulaire Options avancées

Champ	Description
Durée de vie du jeton d'accès	Durée (en secondes) pendant laquelle le jeton d'accès OAuth reste valide avant son expiration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La valeur par défaut est de 1 800 secondes.
Durée de vie du jeton d'actualisation	Durée (en secondes) pendant laquelle le jeton d'actualisation OAuth reste valide avant son expiration. **Remarque :** La valeur par défaut est de 8 640 000 secondes.

4. Mettez à jour les champs de texte du formulaire **(facultatif) du périmètre d'authentification** avec les informations appropriées. Le périmètre d'authentification définit le niveau d'accès d'une application à une ressource. Sélectionnez le périmètre d'authentification pour les API REST spécifiques auxquelles vous souhaitez accéder.

Formulaire du périmètre d'authentification

Champ	Description
Périmètre d'authentification	Niveau d'accès qu'une application a à une ressource. Le périmètre d'authentification limite les actions qu'un jeton d'accès peut effectuer sur les API ou les données.
Autorisation de limite	Noms des API pour lesquelles vous souhaitez restreindre l'autorisation.

   a. Sélectionnez **Créer un nouveau périmètre d'authentification** pour ajouter un nouveau périmètre d'authentification.

5. Sélectionnez **Enregistrer**.
   Un nouveau jeton d'ID de tiers est créé.
6. Accéder à **Tous** > **Intégrations entrantes** > **Registres d'application** pour afficher le jeton d'ID de tiers nouvellement créé.

Octroi de porteur de jeton Web JSON

Utilisez ce flux lorsqu'une application cliente a besoin d'un accès sécurisé et non assisté à des ServiceNow ressources, soit en tant qu'elle-même, soit pour le compte d'un utilisateur.

L'application cliente génère un JWT signé qui inclut les revendications liées à l'identité, telles que l'utilisateur ou le système qu'elle représente. Il l'envoie à l'instance ServiceNow pour demander un jeton d'accès.

JWT Structure

Le JWT doit être signé à l'aide de la clé privée du client. Il doit inclure les allégations standard suivantes :

- iss – Émetteur (ID client)
- sub – Sujet (identité de l'utilisateur ou du système)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- aud – Audience (point de terminaison de jeton ServiceNow)
- exp – Délai d'expiration
- iat – Émis à

Remarque :
ServiceNow utilise la clé publique (chargée dans le profil OAuth JWT) pour valider la signature et mappe la sous-revendication à un enregistrement utilisateur.

Information associée

Workflow d'octroi de jeton Web JSON

Configurer une attribution de porteur de jeton Web JSON OAuth

Workflow d'octroi de jeton Web JSON

Utilisez ce flux lorsqu'une application cliente a besoin d'un accès sécurisé et non assisté à des ServiceNow ressources, soit en tant qu'elle-même, soit pour le compte d'un utilisateur.

Avant de commencer
Rôle requis : oauth_admin, mi_admin, admin

Pourquoi et quand exécuter cette tâche
L'application cliente génère un JWT signé avec des revendications liées à l'identité telles que l'utilisateur ou le système qu'elle représente. L'application cliente envoie le JWT à l'instance pour demander un jeton d'accès ServiceNow .

- **Lorsque vous agissez au nom d'un utilisateur :**

  Le jeton représente un utilisateur précédemment authentifié. Il permet un accès sécurisé et transparent sans avoir à demander à l'utilisateur des informations d'identification ou son consentement. ServiceNow Fait confiance à la demande en validant l'identité de l'utilisateur à partir du jeton signé, éliminant ainsi le besoin d'interaction en temps réel de l'utilisateur.

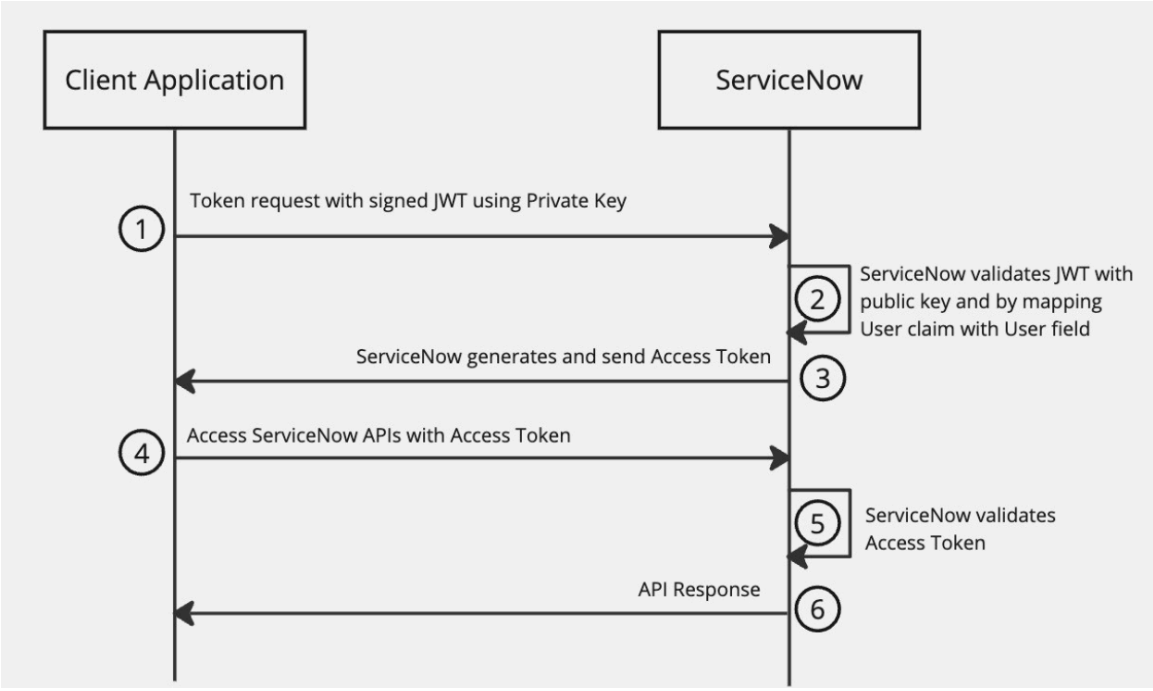
- **Lorsqu'il agit en son propre nom :**

  Le jeton identifie et authentifie l'application cliente. Au lieu d'utiliser un secret partagé, l'application signe le jeton avec une clé privée. Il s'agit d'une alternative plus sécurisée à l'octroi d'informations d'identification du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow d'octroi JWT



Procédure

1. L'application cliente envoie une demande de jeton à ServiceNow, avec un JWT signé avec sa clé privée.
2. ServiceNow valide le JWT à l'aide de la clé publique correspondante.
   Il mappe la revendication `de sous-objet` (objet) dans le jeton à un enregistrement `sys_user` .
3. ServiceNow valide le JWT et émet le jeton d'accès.
4. Le client inclut le jeton d'accès dans les demandes d'API vers ServiceNow.
5. ServiceNow valide le jeton d'accès et renvoie la réponse API appropriée.

Configurer une attribution de porteur de jeton Web JSON OAuth

La configuration d'une attribution titulaire de jeton Web JSON OAuth (JWT) sécurise l'authentification basée sur un jeton sans interaction de l'utilisateur. Il renforce la sécurité avec des JWT signés et réduit les frais généraux d'authentification en éliminant les tentatives de connexion répétées.

Avant de commencer

Rôle requis : `oauth_admin`, `mi_admin`, `admin`

Les algorithmes pris en charge pour JSON Web Token (JWT) : RS256, RS384, RS512, ES256, ES384, ES512.

Procédure

1. Accédez à la **Console des identités des machines** > > **Intégrations entrantes** > > **Nouvelle intégration** > **Attribution du porteur JWT**.
2. Mettez à jour les champs de texte du formulaire Détails avec les informations appropriées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Détails

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès à OAuth JWT.
ID client	ID unique de l'application généré automatiquement. Le système utilise la valeur de ce champ pour récupérer la clé publique ou partagée et valider le JWT. La valeur de ce champ doit correspondre à la valeur des réclamations de l'émetteur et de l'audience dans le JWT.
Secret client	Chaîne secrète partagée que l'instance et l'application cliente ou le site Web utilisent pour autoriser les communications entre eux. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, sélectionnez l'icône de verrouillage.
Champ d'utilisateur	Champ de la table Utilisateur (sys_user) que le système utilise pour faire correspondre la valeur de la réclamation en question dans le JWT. Exemple : Si vous ajoutez un jeton dont la valeur de revendication d'objet est user.name@example.com, vous devez définir le **champ Utilisateur** sur **E-mail**. Ce champ indique au système de rechercher la valeur user.name@example.com dans le champ d'e-mail et d'utiliser l'enregistrement utilisateur correspondant dans la demande entrante.
Activer la vérification JTI	Sélectionnez cette option pour exiger un nouveau jeton à chaque échange de jeton. Par défaut : sélectionné.
URL du JWKS	URL de l'ensemble de clés Web JSON. Il s'agit d'une collection de clés publiques au format JSON. Les fournisseurs d'identité publient un JWKS sur une URL connue afin que les applications et services clients puissent récupérer les clés et valider les signatures des jetons Web JSON (JWT).
Réclamation JTI	Identificateur unique pour chaque jeton. ServiceNow utilise cette réclamation pour détecter et empêcher la relecture d'un jeton en vérifiant qu'un jeton n'est pas réutilisé.
Commentaires	Ajoutez des commentaires pertinents.
Carte de vérificateur JWT	Spécifiez le fournisseur d'identité, la méthode de vérification (telle qu'une URL ou un certificat JWKS) et le mappage des réclamations JWT aux champs d'utilisateur ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Cliquez sur l'icône Plus pour ajouter ou modifier les cartes. Fournissez les détails suivants dans la page de **la carte de vérificateur JWT** : ○ Nom : nom unique de la configuration de la carte de vérificateur JWT. ○ Application : application dans laquelle la carte de vérificateur est utilisée. ○ Enfant (ID de clé) : l'identificateur de la clé utilisée pour valider la signature JWT. ○ Certificat système : enregistrement de certificat ServiceNow utilisé pour la vérification de jeton ○ Clé partagée : clé symétrique utilisée pour valider les jetons.
Actifs	Cochez cette case pour activer l'application OAuth.

3. Mettez à jour les champs de texte du formulaire Options avancées (facultatif) avec les informations appropriées.

Formulaire d'options avancées (facultatif)

Champ	Description
Appliquer la restriction de jeton	Sélectionnez cette option pour activer uniquement l'utilisation des jetons avec les API définies pour activer le profil d'authentification. Vous pouvez définir l'octroi de l'accès à l'aide d'une stratégie d'accès API. Par défaut : non sélectionné.
Durée de vie du cache JWKS	Durée (en minutes) pendant laquelle ServiceNow met en cache le jeu de clés Web JSON (JWKS) à partir du fournisseur d'identité.
Durée de vie du jeton d'accès	Durée (en secondes) pendant laquelle le jeton d'accès reste valide avant son expiration.
Décalage d'horloge	De petites différences dans les horloges système des serveurs ou des appareils impliqués dans la génération et la validation d'un jeton peuvent entraîner des problèmes lors de la validation de réclamations urgentes. Ajustez l'heure ci-dessus. Valeur par défaut : 0 seconde.

4. Mettez à jour les champs de texte du formulaire (facultatif) du périmètre d'authentification avec les informations appropriées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque vous sélectionnez un **périmètre d'authentification**, toutes les API associées sont automatiquement renseignées dans la zone de texte **Limiter l'autorisation** .

Formulaire du périmètre d'authentification

Champ	Description
Périmètre d'authentification	Niveau d'accès d'une application. Le périmètre d'authentification limite les actions qu'un jeton d'accès peut effectuer sur les API ou les données.
Autorisation de limite	Noms des API pour lesquelles vous souhaitez restreindre l'autorisation.

a. Sélectionnez **Ajouter une autre ligne** pour ajouter des champs d'application d'authentification.

b. Sélectionnez **Créer un nouveau périmètre d'authentification** pour ajouter un nouveau périmètre d'authentification.
Entrez le nom du périmètre d'authentification dans la zone de texte **du champ Périmètre** pour sélectionner le périmètre d'authentification nouvellement créé. Vous pouvez ajouter et modifier manuellement les API qui doivent être associées au nouveau périmètre d'authentification.

Remarque :
L'ajout ou la modification d'API à partir du menu **Champ d'application d'authentification** affecte toutes les entités OAuth associées au même périmètre d'autorisation.

5. Sélectionnez **Enregistrer**.
Une nouvelle attribution de porteur de jeton Web JSON OAuth est créée.
6. Accéder à **Tous** > **Intégrations entrantes** > **Registres d'application** pour afficher la subvention de porteur JWT nouvellement créée.

Attribution des informations d'identification du mot de passe de propriétaire de ressource

La configuration d'une attribution d'informations d'identification du mot de passe du propriétaire de ressource OAuth (ROPC) permet aux applications d'authentifier les utilisateurs en utilisant directement leurs informations d'identification pour obtenir un jeton d'accès.

Considérations de sécurité

Le flux ROPC expose les informations d'identification de l'utilisateur directement à l'application cliente, ce qui le rend intrinsèquement moins sécurisé que les alternatives modernes. Elle ne doit être utilisée que dans des scénarios où le client bénéficie d'une confiance totale, d'un contrôle étroit et d'une gestion sécurisée.

Évitez d'utiliser cette subvention dans les applications modernes, sauf en cas d'absolue nécessité. Pour un accès sécurisé basé sur l'utilisateur, il est fortement recommandé d'utiliser le flux de code d'autorisation avec PKCE, qui empêche les informations d'identification d'entrer dans le client et exploite les pratiques de redirection sécurisée et de gestion des jetons.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Workflow d'attribution des informations d'identification du mot de passe de propriétaire de ressource

Configurer un accord d'informations d'identification du mot de passe du propriétaire de ressource OAuth

Workflow d'attribution des informations d'identification du mot de passe de propriétaire de ressource

Ce flux est utilisé dans les environnements hérités ou hautement contrôlés où des alternatives sécurisées ne sont pas possibles. L'application cliente collecte et envoie directement les informations d'identification de l'utilisateur ServiceNow pour obtenir un jeton d'accès, ce qui la rend adaptée uniquement à un usage interne approuvé.

Avant de commencer

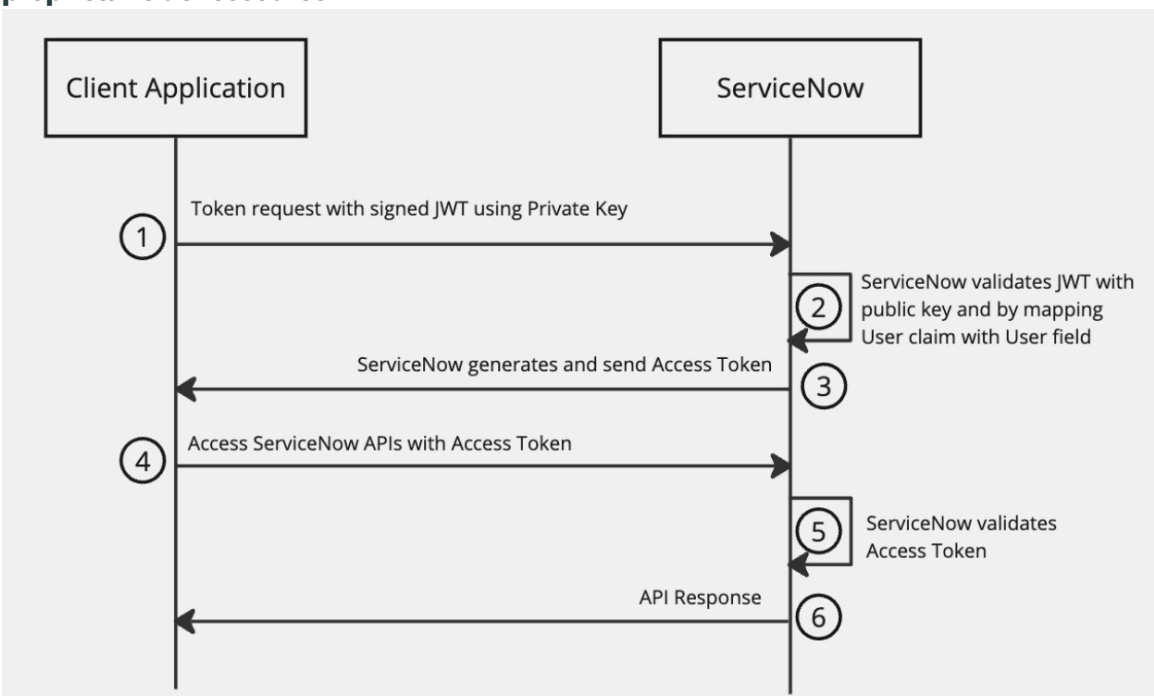
Rôle requis : oauth_admin, mi_admin, admin

Pourquoi et quand exécuter cette tâche

Cette procédure décrit comment une application cliente approuvée obtient un jeton d'accès en gérant directement les informations d'identification de l'utilisateur et l'utilise pour accéder aux API ServiceNow.

L'utilisateur se connecte via l'application, qui envoie ses propres informations d'identification et celles de l'utilisateur à ServiceNow. ServiceNow valide les informations d'identification et émet un jeton d'accès que l'application utilise pour appeler des API.

Workflow d'attribution des informations d'identification du mot de passe de propriétaire de ressource



Procédure

1. L'utilisateur se connecte à l'application cliente.
2. L'application cliente envoie une demande de jeton à avec les paramètres suivants :
   - ID client et secret client.
   - Nom d'utilisateur et mot de passe de l'utilisateur.

Exemple

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Paramètres de demande de jeton

Paramètre	Obligatoire	Description
grant_type	Oui	Spécifie le type d'accord OAuth.
client_id	Oui	L'identificateur unique pour votre application cliente. Format : YOUR_CLIENT_ID
client_secret	Oui	Clé secrète de l'application cliente. Format : YOUR_CLIENT_SECRET
nom d'utilisateur	Oui	Le nom d'utilisateur de l'utilisateur ServiceNow .
mot de passe	Oui	Le mot de passe de ServiceNow l'utilisateur.
scope	Facultatif	Définit le niveau d'accès demandé. Exemple : ○ incident_read ○ incident_write

3. ServiceNow valide les informations d'identification du client et de l'utilisateur, et renvoie le jeton d'accès.
4. Le client utilise le jeton d'accès pour appeler les API ServiceNow.

Exemple

```
Method: GET
Endpoint: https://<servicenow_base_url/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

5. ServiceNow valide le jeton d'accès et renvoie la réponse API.

Configurer un accord d'informations d'identification du mot de passe du propriétaire de ressource OAuth

La configuration d'une attribution d'informations d'identification du mot de passe du propriétaire de ressource OAuth (ROPC) permet aux applications d'authentifier les utilisateurs en utilisant directement leurs informations d'identification pour obtenir un jeton d'accès. Cette méthode est idéale pour les applications approuvées et les systèmes hérités qui nécessitent une authentification sans flux basés sur un navigateur, ce qui permet une validation sécurisée des jetons et un accès contrôlé à l'API.

Avant de commencer

Rôle requis : oauth_admin, mi_admin, admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Console des identités des machines** > > **Intégrations entrantes** > > **Nouvelle intégration** > **Attribution des informations d'identification du mot de passe du propriétaire de ressource OAuth**.
2. Mettez à jour les champs de texte du formulaire **Détails** avec les informations appropriées.

Formulaire Détails

Champ	Description
Nom	Nom fourni par le propriétaire de ressource (utilisateur) lors de l'authentification.
ID client	ID unique affecté pour identifier l'application.
Secret client	Clé secrète que seules l'application et le serveur d'autorisation peuvent identifier. L'application utilise cette clé pour s'authentifier et obtenir des jetons d'accès.
Actifs	Cochez cette case pour activer l'application OAuth.

3. Mettez à jour les champs de texte du formulaire **Options avancées (facultatif)** avec les informations appropriées.

L'application de la restriction de jeton applique des limitations sur la façon dont un jeton d'accès OAuth peut être utilisé, renforçant la sécurité en vérifiant que les jetons ne sont valides que dans des conditions spécifiques. Cochez la case Appliquer la restriction de jeton pour limiter les jetons d'accès OAuth à des API spécifiques définies dans la politique d'accès API. Si l'option Appliquer la restriction de jeton est désactivée, le jeton peut être utilisé dans d'autres API REST.

Formulaire Détails

Champ	Description
Durée de vie du jeton d'accès	Durée (en secondes) pendant laquelle le jeton d'accès reste valide avant son expiration.
Durée de vie du jeton d'actualisation	La durée (en secondes) pendant laquelle un jeton d'actualisation reste valide après son émission est spécifiée dans le champ Durée de vie.

4. Mettez à jour les champs de texte du formulaire (facultatif) du périmètre d'authentification avec les informations appropriées. Le périmètre d'authentification définit le niveau d'accès d'une application à une ressource. Sélectionnez le périmètre d'authentification pour les API REST spécifiques auxquelles vous souhaitez accéder.

Remarque :
Lorsque vous sélectionnez un **périmètre d'authentification**, toutes les API associées sont automatiquement renseignées dans la zone de texte **Limiter l'autorisation** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire du périmètre d'authentification

Champ	Description
Périmètre d'authentification	Niveau d'accès d'une application. Le périmètre d'authentification limite les actions qu'un jeton d'accès peut effectuer sur les API ou les données.
Autorisation de limite	Noms des API pour lesquelles vous souhaitez restreindre l'autorisation.

Remarque :
L'ajout ou la modification d'API à partir du menu **Champ d'application d'authentification** affecte toutes les entités OAuth associées au même périmètre d'autorisation.

a. Sélectionnez **Créer un nouveau périmètre d'authentification** pour ajouter un nouveau périmètre d'authentification.

5. Sélectionnez **Ajouter une autre ligne** pour créer un autre périmètre d'authentification avec les API associées.
6. Sélectionnez **Enregistrer**.
   Une nouvelle attribution des informations d'identification du mot de passe du propriétaire de ressource OAuth est créée.
7. Accéder à **Tous** > **Intégrations entrantes** > **Registres d'application** pour afficher l'attribution des informations d'identification du mot de passe du propriétaire de ressource OAuth nouvellement créée.

Ancienne expérience d'intégrations entrantes

Ancienne expérience : intégrations entrantes.

Remarque :

Vous pouvez effectuer la configuration entrante OAuth en fonction du type de type d'accord suivant :

- Flux d'octroi du code d'autorisation OAuth

  Remarque :
  Pour le flux du code d'autorisation, l'utilisateur doit terminer l'authentification par connexion locale, SSO ou MFA, puis donner son consentement.

- Attribution du mot de passe
- Flux de subvention titulaire JWT
- Flux de jetons d'ID
- Attributions implicites OAuth
- Informations d'identification du client

Configurez l'intégration OAuth qui inclut les améliorations suivantes à partir de la version Zurich :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Augmentez la longueur du secret client jusqu'à 4 096 caractères pour répondre aux exigences de sécurité des systèmes tiers.
- Fournissez une URL JSON Web Key Set (JWKS) pour gérer et mettre à jour automatiquement la clé publique pour la validation de signature des jetons Web JSON (JWT).
- Demandez des jetons OAuth à l'aide du type d'accord JWT signé avec les algorithmes de signature de l'algorithme de signature numérique de courbe elliptique (ES), notamment ES256, ES384 et ES512, pour les jetons Web JSON entrants (JWT).
- Personnalisez le nom de la réclamation JWT ID (JTI) dans les flux entrants OpenID Connect (OIDC) et JWT Bearer.

Flux d'octroi du code d'autorisation OAuth

Le flux d'attribution du code d'autorisation permet à un utilisateur d'accéder à une ressource en s'authentifiant directement auprès d'un serveur OAuth qui fait confiance à la ressource, contrairement à l'authentification avec les informations d'identification nom d'utilisateur/mot de passe.

Cette implémentation du flux de code d'autorisation OAuth permet d'accéder à une ressource via REST. Le cadre de travail du code d'autorisation obtient le jeton d'accès via l'URL autorisée que l'utilisateur configure au lieu de lui demander de saisir un nom d'utilisateur/mot de passe. Le nom d'utilisateur/mot de passe n'est jamais exposé au client qui demande l'accès à la ressource.

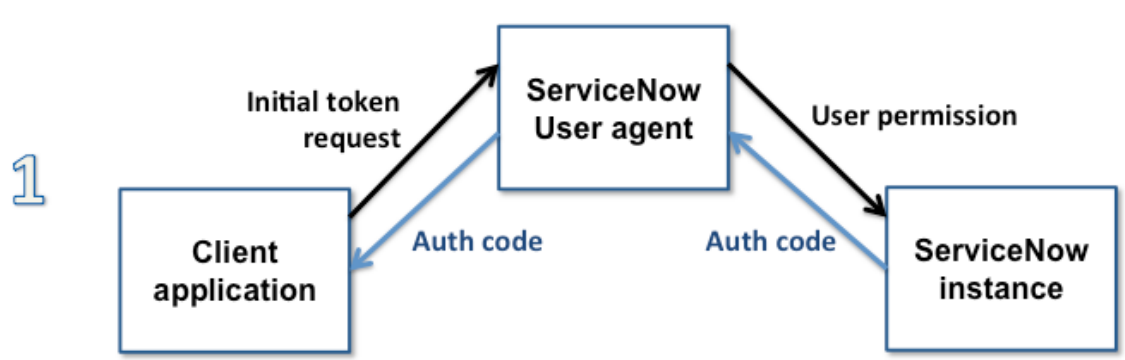
Une ServiceNow instance en tant que serveur d'autorisation

Le serveur OAuth est généralement un serveur d'autorisation tiers. Vous pouvez également spécifier une ServiceNow instance en tant que serveur d'autorisation qui émet les jetons pour le flux de code d'autorisation.

L'utilisateur propriétaire de la ressource restreinte doit autoriser l'accès. L'utilisateur peut également révoquer le jeton d'accès émis à tout moment pour mettre fin à l'accès.

Processus de flux d'octroi du code d'autorisation

Le processus de flux d'octroi du code d'autorisation comprend les trois étapes suivantes :



Dans la première étape, l'application cliente ou le site Web lance un appel d'API REST sous la forme d'une demande GET à l'instance via l'agent utilisateur. En règle générale, l'appel REST est lancé lorsque l'utilisateur final clique sur un bouton ou un lien sur l'application ou le site Web du client pour demander un jeton d'accès. Dans l'application cliente, l'utilisateur final doit également spécifier l'URL d'autorisation, l'URL de jeton, l'ID client et la clé secrète client. Pour obtenir une explication de ces éléments, consultez les descriptions des champs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans cette rubrique : Utiliser un fournisseur OAuth tiers . Si le client demande un type d'accord, l'utilisateur final doit sélectionner Code **d'autorisation**.

Exemple de demande GET de l'application cliente vers l'instance :

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Remarque :
Le **response_type** doit être **un code** pour utiliser le flux d'octroi de code OAuth standard.

L'utilisateur final doit autoriser manuellement l'accès à la ressource restreinte sur l'instance. Dans l'implémentation ServiceNow , l'utilisateur final doit être connecté à l'instance. L'instance invite l'utilisateur final avec une page d'interface utilisateur comportant des boutons **Autoriser** et **Refuser** .

L'élément auprès duquel l'application cliente demande réellement le jeton est l'enregistrement de registre d'application du fournisseur OAuth que vous avez créé, également appelé point de terminaison d'autorisation (voir Utiliser un fournisseur OAuth tiers). Le code d'authentification est envoyé du point de terminaison d'autorisation au client. Il ne va pas directement au client, mais à **l'URL de redirection** que vous spécifiez sur le formulaire de point de terminaison d'autorisation. Cette URL est également connue sous le nom d'URL de rappel. Vous pouvez obtenir cette URL à partir de l'application cliente ou du site Web.

Exemple de réponse de l'instance à l'application cliente, fournissant un code d'autorisation :

```
https/http://{callbackURL}?code={the actual auth code}
```



Maintenant que l'application cliente dispose du code d'autorisation, le client utilise le code pour demander le jeton d'accès. Le code d'autorisation prouve que l'utilisateur a consenti à l'étape 1.

Exemple de demande POST de l'application cliente à l'instance ServiceNow qui fournit le code d'authentification et demande le jeton d'accès :

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorization_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

Le point de terminaison de l'instance renvoie un jeton d'accès et un jeton de rafraîchissement. Le jeton d'actualisation peut être utilisé pour demander des jetons d'accès supplémentaires.

Vous pouvez gérer les jetons, y compris la révocation des jetons, dans l'instance. Consultez Gérer les jetons OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'application cliente utilise le jeton d'accès pour s'authentifier auprès de l'API REST. Après avoir authentifié l'application cliente, l'API REST renvoie les données demandées dans une charge utile JSON.

Exemple de demande GET pour la charge utile JSON de données pour la table Incident [incident] :

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

Remarque :
Le système prend également en charge les octrois implicites OAuth, également appelés flux de code d'octet implicite.

Assistance à l'intégration

Le flux de code d'autorisation prend en charge les intégrations suivantes sur l'instance :

- Authentification unique (SSO) de plusieurs fournisseurs
- Mise à jour SAML 2.0 1
- Authentification multifacteur

L'interface mobile est également prise en charge.

Autoriser l'accès à un point de terminaison OAuth à l'aide du flux de code d'authentification

Les utilisateurs finaux qui possèdent une ressource protégée sur l'instance ServiceNow doivent autoriser l'accès à la ressource avant que l'instance puisse fournir le jeton d'accès.

Avant de commencer
Rôle requis : aucun. Vous devez déjà être connecté à l'instance qui détient la ressource protégée. Vous pouvez également vous connecter à l'aide de la méthode d'authentification (telle que l'authentification multifacteur ou SAML) déjà configurée par votre ServiceNow administrateur.

Procédure

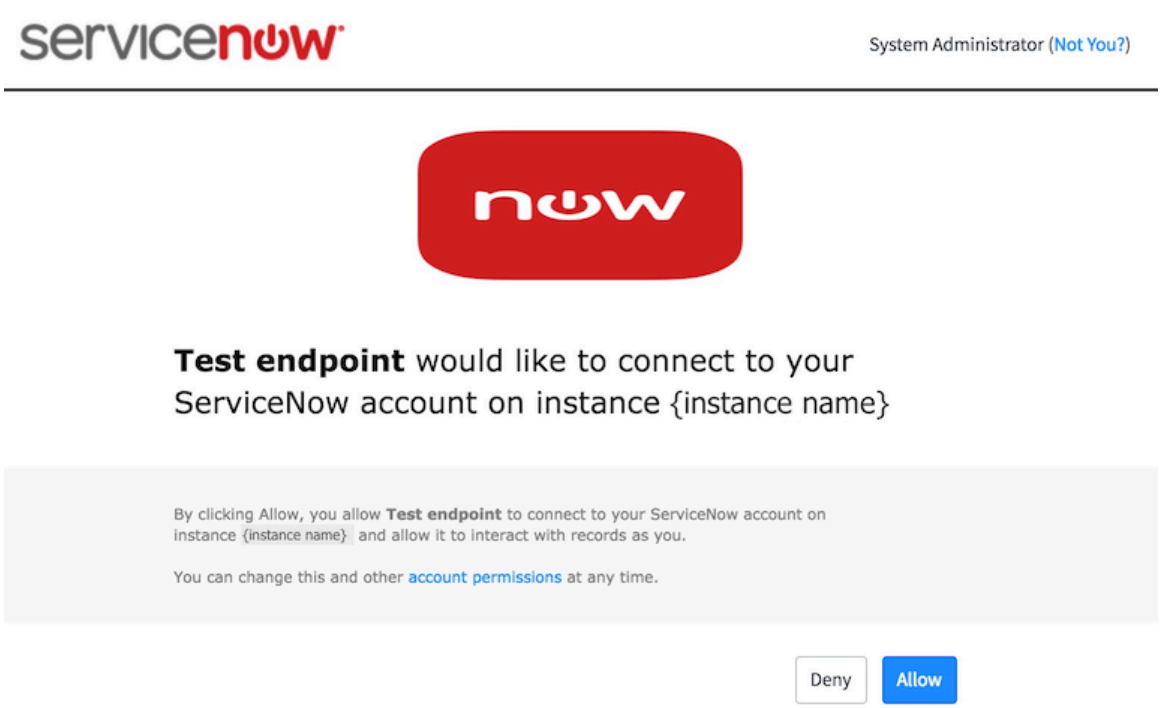
1. Cliquez sur le lien ou le bouton de l'application cliente où vous demandez l'accès à la ressource protégée sur l'instance.
   Cela lance la demande de jeton. Si vous effectuez un appel REST d'une instance à une autre, ce lien est **Obtenir le jeton OAuth** sur le formulaire de message REST.
2. Si vous n'êtes pas connecté, connectez-vous maintenant.
   Si vous n'êtes pas le même utilisateur que celui spécifié dans l'angle supérieur droit, cliquez sur **Ce n'est pas vous ?** et connectez-vous.
3. Cliquez sur autorisations du compte pour ouvrir la liste des jetons d'accès que vous avez déjà émis.
   C'est la même chose que le **Libre-service** > **Mes connexions** Liste de jetons d'applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Autoriser** pour autoriser l'accès et demander à l'instance d'émettre le code d'autorisation (si vous utilisez le flux de code d'authentification) ou le jeton d'accès (si vous utilisez le type d'accord implicite).

   Si vous cliquez sur **Refuser**, l'autorisation n'est pas autorisée, mais vous n'êtes pas déconnecté de l'instance.



   Un message confirmant l'accès doit s'afficher. Si vous demandez l'accès à partir du formulaire de message REST sur une instance, le message suivant s'affiche en haut du formulaire : Le jeton d'actualisation OAuth est disponible et expirera à {date}.

Exigence de paramètre d'état de flux du code d'autorisation

La propriété système glide.oauth.state.paramater.required permet d'exiger le paramètre État dans une demande OAuth pour le flux de code d'autorisation.

Paramètre d'état

Rôle requis : aucun.

À partir de la version Madrid, la propriété *`glide.oauth.state.parameter.required`* système ajoute un paramètre d'état pour une demande OAuth. Pour les instances zbooted, la propriété est true. Pour les instances mises à niveau, la propriété n'est pas présente, le paramètre État n'est donc pas activé. Le paramètre State est une valeur de chaîne et ne doit pas contenir de caractères spéciaux. Le paramètre État ne peut pas être vide ou « ».

Validation du paramètre d'état

Créez un point de terminaison pour permettre aux clients d'accéder à l'instance. Lancez un flux de code d'autorisation pour un oauth_auth.do. Par exemple :

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=
e9dba45b380d1300e676ccc91cef468f&response_type=code
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous ne spécifiez pas le paramètre d'état dans la demande, vous obtenez une erreur et le code d'autorisation n'est pas renvoyé.Paramètre d'état manquant dans la demande.

Ajout du paramètre d'état à la demande :

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=
e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

L'ajout du paramètre État vous redirige vers l'écran de connexion et le flux de code d'autorisation habituel renvoie le code d'autorisation.

Remarque :
L'URL de réponse contient le paramètre d'état transmis dans la demande. Dans l'exemple, le paramètre ajouté est `state=123`.

Si le flux du code d'autorisation commence à partir de oauth_initiator.do :

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_mes
sage&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fe
c0d1300964f214a2c2fcf51&response_type=code
```

Le paramètre État est automatiquement ajouté lorsqu'il est redirigé par oauth_auth.do.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&r
edirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc9
1cef468f
```

Exemple de flux de code d'autorisation : ServiceNow instance en tant que serveur d'autorisation

Vous pouvez utiliser une instance comme serveur d'autorisation pour émettre des jetons à un client à l'aide du flux de code d'autorisation.

Avant de commencer
Rôle requis : aucun.

Cet exemple utilise deux instances : l'une en tant que serveur d'autorisation et l'autre en tant que client. Une instance utilise un appel REST pour demander des jetons à une autre instance.

Vous devez le faire Activer OAuth dans les deux cas.

Procédure

1. Sur l'instance de serveur d'autorisation (exécutant la version Istanbul ou ultérieure), accédez à **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**.
3. Renseignez les champs de formulaire de l'enregistrement d'application OAuth comme décrit dans Créer un point de terminaison pour permettre aux clients d'accéder à l'instance.
   La réalisation de ces étapes configure un serveur d'autorisation. Suivez les étapes suivantes pour configurer le serveur client.
4. Sur l'instance client, accédez à **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
5. Cliquez sur **Se connecter à un fournisseur OAuth tiers**.
6. Renseignez les champs de formulaire de l'enregistrement d'application OAuth comme décrit dans .
   Notez les valeurs de champ suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Nom** : nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
- **ID client** : ID client de l'enregistrement de registre d'application que vous avez créé pour le serveur d'autorisation.
- **Secret client** : [Lecture seule] L'ID unique de l'application généré automatiquement. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
- **Type d'accord par défaut** : sélectionnez **le code d'autorisation**.
- **URL d'autorisation** : URL de l'instance qui est le serveur d'autorisation. N'oubliez pas d'ajouter `oauth_auth.do` à la fin de l'URL.
- **URL du logo** : URL qui contient une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'accès à une application cliente à une ressource restreinte sur l'instance.
- **URL de jeton** : URL de l'instance qui constitue le serveur d'autorisation. N'oubliez pas d'ajouter `oauth_token.do` à la fin de l'URL.
- **URL de redirection** : URL de l'instance : l'instance du serveur client. N'oubliez pas d'ajouter `oauth_redirect.do` à la fin de l'URL.

7. Créez un profil pour l'enregistrement avec le type d'accord **du code d'autorisation** .
   Le serveur client est configuré. Vous pouvez maintenant créer un message REST sortant et obtenir un jeton OAuth.

Créer un point de terminaison pour permettre aux clients d'accéder à l'instance

Créez un point de terminaison d'application OAuth pour permettre aux applications clientes externes d'accéder à l'instance ServiceNow .

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**, puis remplissez le formulaire.

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
ID client	[Lecture seule] ID unique de l'application généré automatiquement. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
Secret client	[Obligatoire] Chaîne secrète partagée que l'instance et l'application cliente ou le site Web utilisent pour autoriser les communications entre eux. L'instance utilise le secret client lorsqu'elle demande un jeton d'accès. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, cliquez sur l'icône de verrouillage.
URL de redirection	URL de rappel vers laquelle le serveur d'autorisation redirige. Entrez les URL complètes des clients demandant l'accès à la ressource, annexées par `/oauth_redirect.do`. Par exemple, `http ://token_consumer :port/oauth_redirect.do`. Saisissez autant d'URL que nécessaire pour tous les consommateurs de jetons possibles. L'instance associe l'URL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de la demande entrante à l'une des URL de redirection. Si aucune correspondance n'est établie, l'instance utilise la première URL de redirection.
URL du logo	URL contenant une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'accès à une application cliente à une ressource restreinte sur l'instance.
Actifs	Cochez cette case pour activer le registre d'application.
Durée de vie du jeton d'actualisation	Nombre de secondes de validité d'un jeton d'actualisation. L'instance utilise la valeur Durée de vie lors de la demande d'un jeton d'actualisation. Par défaut, les jetons d'actualisation expirent dans 100 jours (8640 000 secondes).
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation de jetons avec des API définies pour autoriser le profil d'authentification. Vous pouvez définir l'octroi de l'accès à l'aide d'une stratégie d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Client mobile	Représente l'entité pour l'application mobile ou le Web. Ces informations sont utilisées pour analyser les informations de connexion avec mobile ou web.
Durée de vie du jeton d'accès	Nombre de secondes pendant lesquelles un jeton d'accès est valide. L'instance utilise la valeur Durée de vie lors de la demande d'un jeton d'accès. Par défaut, les jetons d'accès expirent au bout de 30 minutes (1 800 secondes).
Format du jeton	Format du jeton à générer. Le format détermine la structure d'un jeton et les informations qu'il contient.
Réclamation de sujet	Champ de la table Utilisateur (sys_user) utilisé pour renseigner la valeur de l'objet (sous-)réclamation d'un jeton JWT. La sous-revendication est un élément d'information qui identifie le sujet, ou l'utilisateur, du jeton JWT. Ce champ s'applique uniquement si le **format de jeton** est JWT.
Commentaires	Informations supplémentaires à associer à l'application.
Type de client	Choisissez le type de client, en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

3. Cliquez sur **Envoyer**.

Résultats

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type Client OAuth. Lorsque l'instance émet réellement des jetons et des codes d'autorisation, ils sont stockés dans la table. Pour plus d'informations , consultez Gérer les jetons OAuth .

Paramètres de réponse de l'API OAuth

L'API OAuth 2.0 produit une réponse JSON contenant les paramètres suivants sous forme de paires nom-valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de réponse du jeton d'accès

Paramètre de réponse	Description
périmètre	Quantité d'accès accordée par le jeton d'accès. Le champ d'application est toujours **useraccount**, ce qui signifie que le jeton d'accès a les mêmes droits que le compte d'utilisateur qui a autorisé le jeton. Par exemple, si Abel Tuter autorise une application en fournissant des informations d'identification de connexion, le jeton d'accès résultant accorde au porteur du jeton les mêmes privilèges d'accès qu'Abel Tuter.
token_type	Type de jeton émis par la demande tel que défini dans la RFC OAuth. Le type de jeton est toujours **Bearer**, ce qui signifie que toute personne en possession du jeton d'accès peut accéder à une ressource protégée sans fournir de clé cryptographique. Consultez RFC6750 pour plus d'informations sur la façon dont OAuth 2.0 utilise les jetons de porteur.
expires_in	Durée de vie du jeton d'accès en secondes.
refresh_token	Valeur de chaîne du jeton d'actualisation.
access_token	Valeur de chaîne du jeton d'accès. Les demandes d'accès effectuées pendant le délai d'expiration du jeton d'accès renvoient toujours le jeton d'accès actuel.
format	[Facultatif] Format de sortie de la réponse. Cette valeur est toujours au format JSON.

Remarque :
Si un fournisseur OAuth envoie le corps de la réponse sous la forme « type-contenu » au lieu de « type-contenu », le client HTTP OAuth peut ne pas analyser la réponse correctement. Pour corriger ce problème, créez une propriété système à l'aide de ces paramètres.

Champ	Valeur
Nom	glide.oauth.inhouse.httpclient.enabled
Type	true|false
Valeur	Faux

Pour plus d'informations sur la création de propriétés système, voir Ajouter une propriété système

L'exemple suivant illustre la chaîne JSON renvoyée par une demande de jeton d'accès. (Des espaces ont été ajoutés pour améliorer la lisibilité).

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyxshU9mMQ13gJHtxD2fy"}
```

Paramètres de demande de l'API OAuth

Découvrez les paramètres de demande d'API OAuth utilisés par les demandes de jeton d'accès.

Remarque :
Le type de contenu de l'API OAuth doit être `application/x-www-form-urlencoded`. Un type de contenu `application/json` entraîne une erreur non spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de demande de jeton d'accès

Paramètre de demande	Description
grant_type	[Obligatoire] Type d'informations d'identification autorisant la demande d'un jeton d'accès. Ce paramètre doit avoir l'une des valeurs suivantes : • **mot de passe** : ensemble des informations d'identification de l'utilisateur pour autoriser la demande de jeton d'accès. Spécifiez les informations d'identification de l'utilisateur dans les paramètres nom d'utilisateur et mot de passe. • **refresh_token** : un jeton d'actualisation existant autorise la demande de jeton d'accès. Spécifiez le jeton d'actualisation dans le paramètre refresh_token.
client_id	[Obligatoire] ID unique généré automatiquement de l'application cliente demandant le jeton d'accès.
client_secret	[Obligatoire] Chaîne secrète partagée que l'instance et l'application OAuth utilisent pour autoriser les communications l'une avec l'autre.
nom d'utilisateur	Nom du compte utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jeton d'accès avec une **grant_type** de **mot de passe**.
mot de passe	Mot de passe du compte utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jeton d'accès avec une **grant_type** de **mot de passe**.
refresh_token	Jeton d'actualisation existant qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jeton d'accès avec un **grant_type** de **refresh_token**.

Demandes utilisant les informations d'identification de l'utilisateur

L'instance exige que les clients fournissent des informations d'identification de connexion lors de l'autorisation initiale du client ou lors de l'autorisation de la création d'un jeton d'actualisation. Ce type de demande renvoie toujours deux jetons :

- Un jeton d'accès
- Un jeton d'actualisation

L'instance vérifie que l'utilisateur est actif, qu'il n'est pas actuellement verrouillé et qu'il dispose d'une session interactive. Si l'une de ces conditions est fausse, l'instance ne produit pas de jeton d'accès. Les demandes d'accès effectuées dans le délai d'expiration du jeton d'accès renvoient toujours le jeton d'accès actuel.

Remarque :
Ce type d'octroi d'autorisation s'appuie sur le chiffrement TLS pour protéger les informations d'identification de l'utilisateur pendant la transmission.

L'exemple suivant illustre la demande d'un jeton d'accès avec un ensemble d'informations d'identification d'utilisateur (des espaces ont été ajoutés pour améliorer la lisibilité).

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demandes utilisant un jeton d'actualisation

L'instance peut utiliser un jeton d'actualisation existant pour créer un nouveau jeton d'accès. Ce type de demande renvoie uniquement un jeton d'accès. L'instance confirme que le jeton d'actualisation n'a pas expiré avant de générer un nouveau jeton d'accès. Les demandes d'accès effectuées pendant le délai d'expiration du jeton d'actualisation renvoient toujours le jeton d'actualisation actuel. La transmission des jetons de rafraîchissement est généralement plus sécurisée que la transmission des informations d'identification de l'utilisateur. L'exemple suivant illustre la demande d'un jeton d'accès avec un jeton de rafraîchissement existant (des espaces ont été ajoutés pour améliorer la lisibilité).

```
$ curl -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Créer un point de terminaison d'API JWT OAuth pour les clients externes (intégration de machine à machine)

Le jeton de porteur OAuth JWT permet aux applications Web clientes de s'authentifier auprès de votre instance de manière transparente à l'aide du type d'accord JWT entrant au lieu de demander à l'utilisateur final de se connecter manuellement ou de partager le mot de passe.

Avant de commencer

Les algorithmes pris en charge pour JSON Web Token (JWT) : RS256, RS384, RS512, ES256, ES384, ES512.

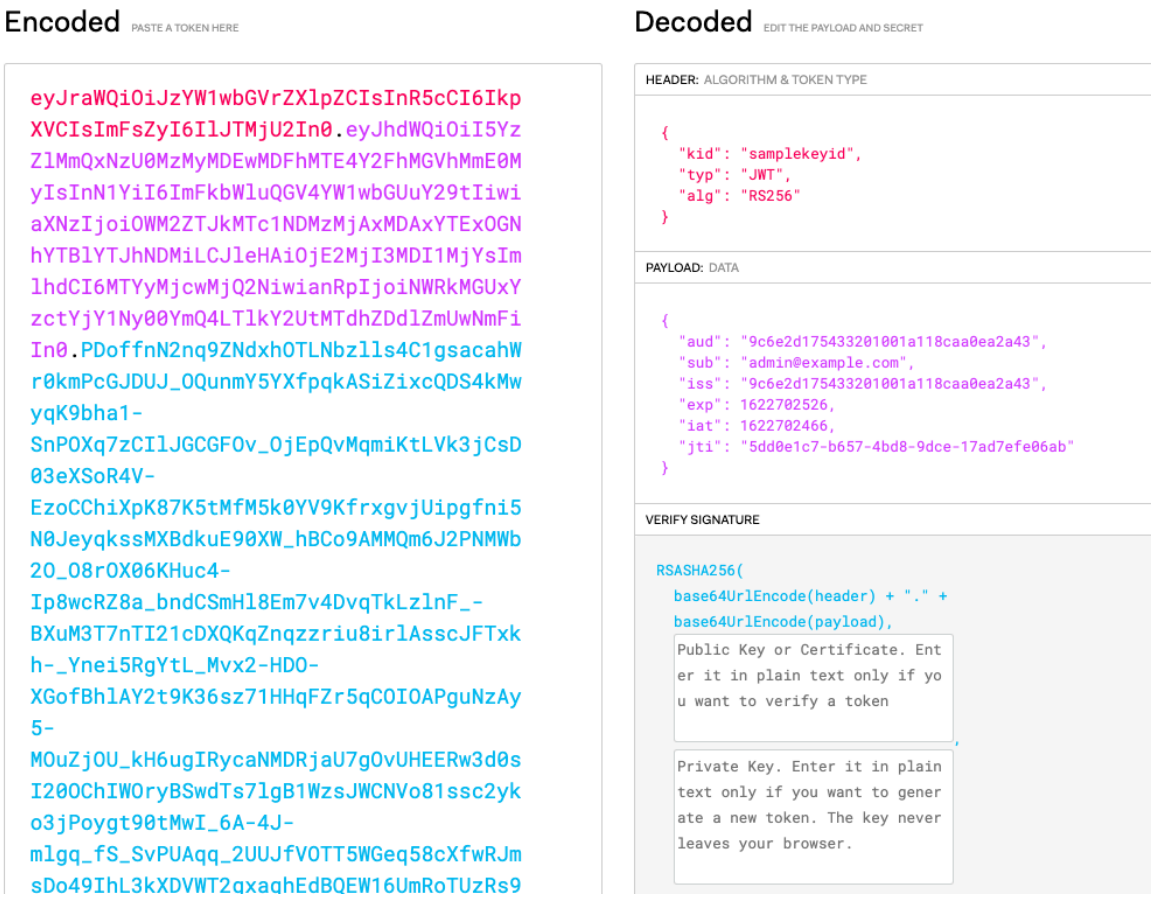
Générer un JWT avec les revendications suivantes côté client :

- `aud` : doit correspondre à la valeur de l'ID client.
- `sub` : doit être un identificateur utilisateur, tel que l'e-mail de l'utilisateur auquel vous souhaitez associer le jeton.
- `iss` : correspondance recommandée avec la valeur de l'ID client. Si l'`aud` et l'`iss` ne correspondent pas, ajoutez la valeur `iss` dans la validation de la réclamation.
- `exp` : toute expiration souhaitée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de jeton Web JSON décodé



Configuration dans ServiceNow

Pourquoi et quand exécuter cette tâche

Étant donné que l'utilisation du type d'accord JWT n'inclut pas le mot de passe dans la demande, elle permet une plus grande sécurité entre les services web. Par exemple, vous pouvez développer une application externe et utiliser des jetons pour authentifier les demandes entrantes envoyées à votre ServiceNow instance.

Rôle requis : admin

Pour plus d'informations sur les jetons Web JSON, reportez-vous à la section https://jwt.io/ .

Procédure

1. Ajoutez la clé publique de l'application cliente à la table **sys_certificate** .
2. Configurez la configuration dans votre ServiceNow instance pour vérifier le JWT entrant.
   a. Accédez à la **OAuth système** > **Registre d'application**.
   b. **Sélectionnez Créer un point de terminaison d'API JWT OAuth pour les clients externes**.
   c. Remplissez le formulaire avec les informations relatives à votre jeton.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table OAuth JWT

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès à OAuth JWT.
ID client	ID unique de l'application généré automatiquement. Le système utilise la valeur de ce champ pour récupérer la clé publique ou partagée et valider le JWT. La valeur de ce champ doit correspondre à la valeur des réclamations de l'émetteur et de l'audience dans le JWT.
Secret client	Chaîne secrète partagée que l'instance et l'application cliente ou le site Web utilisent pour autoriser les communications entre eux. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, sélectionnez l'icône de verrouillage. **Remarque :** Si **Client public** est sélectionné, vous pouvez omettre le **secret client**.
Champ d'utilisateur	Champ de la table Utilisateur (sys_user) que le système utilise pour faire correspondre la valeur de la réclamation en question dans le JWT. Par exemple, si vous ajoutez un jeton dont la valeur de réclamation d'objet est user.name@example.com, vous devez définir le **champ Utilisateur** sur **E-mail**. Ce champ indique au système de rechercher la valeur user.name@example.com dans le champ d'e-mail et d'utiliser l'enregistrement utilisateur correspondant dans la demande entrante.
Activer la vérification JTI	Sélectionnez cette option pour exiger un nouveau jeton à chaque échange de jeton. Par défaut : sélectionné.
Application	Champ d'application de l'application en lecture seule. Ce champ est renseigné automatiquement.
Accessible depuis	Politique d'accès entre périmètres. Pour plus d'informations, consultez Paramètres d'accès à l'application .
Durée de vie du jeton d'accès	Durée de validité du jeton. Unité : Secondes
Format du jeton	Format du jeton à générer. Le format détermine la structure d'un jeton et les informations qu'il contient.
Réclamation de sujet	Champ de la table Utilisateur (sys_user) utilisé pour renseigner la valeur de l'objet (sous-)réclamation d'un jeton JWT. La sous-revendication est un élément d'information qui identifie le sujet, ou l'utilisateur, du jeton JWT. Ce champ s'applique uniquement si le **format de jeton** est JWT.
Décalage d'horloge	Différence de temps autorisée entre les horloges serveur et client lors de la validation des réclamations exp et nbf dans JWT. Unité : Secondes Par défaut : 300

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Appliquer les restrictions de jeton	Sélectionnez cette option pour activer uniquement l'utilisation des jetons avec les API définies pour activer le profil d'authentification. Vous pouvez définir l'octroi de l'accès à l'aide d'une stratégie d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Commentaires	Informations supplémentaires à associer à l'application.
Client public	Ajoutez ce champ au formulaire si le client JWT est public. Lorsque cette option est sélectionnée, vous n'avez pas besoin d'inclure de **secret client**. Par défaut : non sélectionné.
Type de client	Choisissez le type de client, en fonction du type de votre client. Options : ▪ **iframe incorporé** ▪ **Intégration en tant qu'utilisateur** ▪ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

d. Enregistrez le formulaire.

e. Ajoutez des enregistrements à la liste connexe des cartes de vérificateur JWT pour vérifier la signature JWT.

Table de cartes de vérificateur JWT

Champ	Description
Nom	Nom de l'enregistrement de mappage JWT.
Enfant	ID clé de JWT
Clé partagée	Clé partagée pour l'ID de clé spécifié.
Application	Champ d'application de l'application en lecture seule.
Certificat système	Enregistrement du certificat dans la table Certificats X.509 (sys_certificate). Le certificat qui a été chargé à l'étape 1.

f. Ajoutez toutes les réclamations personnalisées associées à votre JWT à la liste connexe Validations des réclamations OAuth JWT.

Vous n'avez pas besoin d'ajouter d'enregistrements pour les déclarations requises suivantes :

- Iss
- Aud
- sub
- exp

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si l'aud et l'iss ne correspondent pas, ajoutez la valeur iss dans la validation de la réclamation.
- Pour les certificats, vous pouvez ajouter plusieurs cartes de vérificateur associées à plusieurs clés.

Table des validations des réclamations OAuth JWT

Champ	Description
Mon client externe	Rempli automatiquement avec l'enregistrement JWT OAuth.
Type de valeur de réclamation	Type de données de la valeur de réclamation.
Nom de la réclamation	Nom de la réclamation que vous souhaitez ajouter.
Valeur de réclamation	Valeur de la réclamation.
Application	Champ d'application de l'application en lecture seule.

3. Envoyez une demande cURL contenant le jeton JWT pour obtenir un jeton d'accès de votre instance.

Example

Voici un exemple de commande cURL demandant un jeton d'accès :

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6uglRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Si le client JWT est un client public, tel que le SDK mobile, vous pouvez omettre les paramètres client_id et client_secret de la demande. Voici un exemple de commande cURL demandant un jeton d'accès qui omet le client_id et client_secret :

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIIJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HfIcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

L'instance renvoie le jeton d'accès dans sa réponse :

```
{
   "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxNA",
   "scope": "useraccount",
   "token_type": "Bearer",
   "expires_in": 1799
}
```

Remarque :
Le type d'accord JWT entrant n'inclut pas les jetons d'actualisation.

4. Effectuez un appel d'API REST pour accéder à une ressource à l'aide du jeton d'accès.

Example

Ce qui suit est une commande cURL permettant d'accéder à la table des incidents à l'aide du jeton.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Résultats
Le système récupère le jeton d'accès dans l'appel REST et active l'accès à la ressource demandée.

Configurer un fournisseur OIDC OAuth pour accepter les jetons tiers

Vous pouvez configurer un fournisseur OIDC OAuth pour qu'il accepte les jetons d'identité générés par un fournisseur OIDC tiers à l'aide d'appels d'API entrants à l'aide de l'option Authentification unique (SSO de plusieurs fournisseurs).

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Prend ServiceNow AI Platform en charge OIDC via notre implémentation Single Sign-On (SSO) externe en plus des appels d'API entrants. Pour obtenir un exemple de configuration de fournisseur OIDC, consultez Configuration d'Azure AD. Pour obtenir un exemple de configuration de fournisseur OIDC spécifique à SSO, consultez Créer une configuration OpenID Connect (OIDC) pour Single Sign-On (SSO).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
   - Sélectionnez **Nouveau**, sélectionnez **Configurer un fournisseur OIDC pour vérifier les jetons d'ID**, puis remplissez le formulaire.
   - Sélectionnez un modèle existant pour un fournisseur OIDC (ADFS, Auth0, Azure AD, Google, Okta), puis remplissez le formulaire.

     Remarque :
     les modèles de fournisseur OIDC sont disponibles après le chargement des données de démonstration avec le module d'extension OAuth 2.0.

Champ	Description
Nom	Nom unique qui identifie l'entité OIDC OAuth.
ID client	L'ID client de l'application enregistré sur le serveur OAuth OIDC tiers. Cette valeur doit être la même que la valeur de la réclamation `aud` dans le jeton JWT.
Script de l'API OAuth	Script que vous pouvez utiliser pour personnaliser les demandes et les réponses adressées à un fournisseur OAuth externe.
Configuration du fournisseur OIDC OAuth	Les fournisseurs OIDC (ADFS, Auth0, Azure AD, Google, Okta) peuvent être utilisés pour valider le jeton JWT. Sélectionnez l'enregistrement de la configuration de votre fournisseur OIDC pour valider que la **réclamation de l'utilisateur** et le **champ de l'utilisateur** sont définis de manière appropriée. Assurez-vous également de remplir les champs suivants : ○ Activer la vérification de la **réclamation JTI** : lorsque cette option est activée, la validation du ServiceNow jeton JWT valide également le JTI envoyé par le fournisseur. ○ **URL des métadonnées OIDC** : détails de la configuration connue du fournisseur OIDC. **Remarque :** Si la validation n'est pas vérifiée, le `JTI` ne peut pas être validé, qu'il soit présent ou non dans le jeton JWT. Le nom de la réclamation dans le jeton doit être `jti`.
Décalage d'horloge	Nombre de secondes, pour que la contrainte soit considérée comme valide. La valeur par défaut est 300.
Appliquer les restrictions de jeton	Sélectionnez cette option pour activer uniquement l'utilisation des jetons avec les API définies pour activer le profil d'authentification. Vous pouvez définir l'octroi de l'accès à l'aide d'une stratégie d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Actif	Cochez cette case pour activer l'application OAuth.
Type de client	Choisissez le type de client, en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

2. Sélectionnez **Soumettre**.
   L'enregistrement est enregistré dans la table Registres d'application [oauth_entity].
   Lorsque votre instance émet des jetons et des codes d'autorisation, elle crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type **Fournisseur OIDC externe**. Consultez pour plus d'informations.
3. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Profils des entités OAuth pour valider un profil par défaut généré par le système pour le nouveau fournisseur OAuth sans aucun champ d'application.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth comprenant le nom, le type d'accord et le périmètre OAuth.
4. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Périmètres des entités OAuth pour définir tous les champs d'application OAuth disponibles pour ce fournisseur OAuth.
   Les champs d'application définis peuvent être sélectionnés lorsque vous créez ou mettez à jour un profil.
   Chaque champ d'application OAuth défini contient un nom et un champ d'application que vous devez obtenir de la spécification du fournisseur, telle qu'un champ d'application en lecture ou en écriture. Chaque périmètre doit être défini séparément.
5. **Facultatif :** Accédez à la liste connexe de l'enregistrement Attribution d'utilisateurs pour activer l'attribution automatique d'utilisateurs.

Option	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer l'authentification forcée pour les utilisateurs.
Mettre en service la source de données	La source de données à utiliser pour transformer un jeton OIDC en utilisateur ServiceNow . Utilisez la **liste de recherche** pour sélectionner le modèle de source de données prédéfini, puis ouvrez l'enregistrement pour configurer le mappage de la table transformée. Lors de la configuration du mappage de transformation, les champs sources proviennent de , `JWT token`les champs cibles sont ceux de la `sys_user` table.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Les rôles d'utilisateur appliqués aux utilisateurs nouvellement mis en ServiceNow service.

Example: Voici un exemple de requête cURL pour invoquer un appel d'API REST

Invoquez un appel d'API REST.

Procédez comme suit :

- Enregistrez l'application dans le fournisseur OpenID Connect.
- Configurez l'entité OIDC OAuth.
- Configurez le fournisseur OIDC :

Fournisseur OIDC

Fournisseur OIDC	Nom du fournisseur OIDC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

URL des métadonnées OIDC	Spécifiez l'URL des métadonnées OIDC (URL de configuration connue). Ces informations sont utilisées pour extraire les clés publiques afin de valider le jeton via le point de terminaison JWKS .
Réclamation de l'utilisateur	La réclamation qui est validée par rapport à la table utilisateur.
Champ d'utilisateur	Réclamation de l'utilisateur qui identifie l'enregistrement utilisateur.
Activer la vérification de la réclamation JTI	Lorsqu'elle est activée, la validation du jeton JWT ServiceNow valide également le JTI envoyé par le fournisseur. **Remarque :** Si la validation n'est pas vérifiée, le JTI ne peut pas être validé, qu'il soit présent ou non dans le jeton JWT. Le nom de la réclamation dans le jeton doit être jti. Ces informations sont utilisées pour prévenir les attaques par relecture.

- Obtenez un jeton JWT.
- Invoquez un appel d'API REST.
  - Jeton d'ID dans l'en-tête d'autorisation pour accéder à l'API de table ou au service Web scripté.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04f2dbd4a300a1
35364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4Iiwi
YWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVtYWlsIjoi
aW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi05MzQ
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2lCT3dwd0IwaDciLCJpYXQiOj
E1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm16SzRs
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMDBvZ
2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5hbW
UiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmFtZSI6I
mFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfYXQiOj
E1Mzc5MzAxOTcsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2Nj
F9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347zvcz
mLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFHk4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51IqxAsXns
0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

  - Si l'utilisateur est authentifié, une réponse application/json valide est renvoyée. Sinon, un message d'erreur utilisateur non authentifié est renvoyé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to provide Auth
 information"},"status":"failure"}
```

Configurer le type de client pour les enregistrements OAuth et SSO

Configurez le champ **Type de client** pour les configurations liées aux enregistrements OAuth et SSO.

Lors de l'établissement de sessions pour différents types de connexion tels que l'interface utilisateur Web (connexion interactive), Iframe incorporé, incorporé ou d'intégration, vous pouvez configurer le type de client pour les enregistrements OIDC (entité OAuth), SAML et Digest qui sont utilisés pour diverses connexions.

Les choix du type de client sont les suivants :

- **Iframe incorporé :** peut être utilisé pour une instance interactive ServiceNow qui réside dans un iframe dans les sites Web tiers. Par exemple, s'il existe une table sensible (table sys_user - numéro de téléphone de l'utilisateur), en tant qu'administrateur, vous pouvez configurer l'ACL avec l'attribut sec (Iframe incorporé) défini sur faux, afin d'éviter que l'utilisateur n'accède aux données (informations de table) sur la session Iframe incorporée dans le tiers.
- **Intégration en tant qu'utilisateur** : peut être utilisé pour le chatbot Agent virtuel installé dans des applications de bureau telles que Slack, Teams...
- **Intégration en tant que service** : peut être utilisé pour l'intégration de machine à machine (communication entre services).

Remarque :

- [store-future: BEGIN review]Le type Embedded as a client est disponible lorsque le module d'extension Embedded client access (com.glide.security.client_access) est installé pour OIDC (OAuth Entity).[End]
- Pour OIDC (entité OAuth) : tous les choix sont disponibles.
- Pour SAML et Digest : uniquement Iframe intégré. Vous devez modifier le formulaire et ajouter le champ **Type de client** à l'enregistrement, puis sélectionner le type de client **Iframe incorporé** .
- Si le **type de client** sélectionné est aucun, il n'y a pas de classification de la session.

Il est recommandé d'utiliser le champ de type client pour tous les enregistrements créés pour OIDC (entité OAuth), SAML et Synthèse. Cela vous permet d'avoir un meilleur contrôle sur chaque méthode de connexion qui a les mêmes configurations mais qui se distingue par le type de client.

Après la configuration du champ, chaque fois qu'un utilisateur se connecte à partir de la configuration correspondante (OAuth ou SSO), une fois l'authentification réussie, la session est considérée en fonction du type de client configuré et, en conséquence, le délai d'expiration de la session est exploité.

Pour la session en cours, l'attribut de sécurité correspondant est inclus ou peut être exploité pour empêcher les utilisateurs d'accéder aux informations spécifiques à la table dans le type de client sélectionné. Pour plus d'informations, consultez Attributs de sécurité OOB (prêts à l'emploi).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Délai d'expiration de la session pour les types de clients

Voici les propriétés système relatives au délai d'expiration de session pour les différents types de clients :

- [store-future: BEGIN review]glide.session_timeout.incorporé[End]
- glide.session_timeout.iframe_embedded
- glide.session_timeout.integration_as_a_user
- glide.session_timeout.integration_as_a_service

Attributions implicites OAuth

ServiceNow Les instances prennent en charge l'octroi implicite d'un jeton d'accès.

Le type d'accord implicite, également connu sous le nom de *`implicit grant code flow`*, permet de donner le jeton d'accès directement à l'application cliente via l'agent utilisateur, qui est généralement le navigateur Web ou l'appareil mobile. Aucun jeton de rafraîchissement n'est accordé. L'utilisateur final doit toujours accorder l'accès à la ressource protégée sur l'instance, comme pour l'instance standard.

Processus de flux d'attribution implicite OAuth

Tout comme pour le processus de flux de code d'autorisation standard, l'application cliente envoie une demande d'utilisation de la ressource restreinte sur l'instance et l'utilisateur final l'approuve. La demande se présente sous la forme d'une URL envoyée à l'instance. L'URL doit inclure les paramètres suivants :

- client_id=<l'ID client nécessaire>. Cette option est obligatoire pour identifier la ressource protégée à laquelle l'application cliente souhaite accéder.
- response_type=jeton. Ceci est obligatoire pour demander le jeton d'accès directement (par opposition à demander un code d'autorisation). La valeur doit être un jeton pour les octrois implicites. Dans l'exemple de flux de code d'autorisation standard, le type de réponse est code.
- redirect_uri=<a URL> : l'emplacement où le jeton est envoyé.

Le serveur d'autorisation envoie le jeton d'accès, plutôt qu'un code d'autorisation, à l'application cliente via l'agent utilisateur.

Voici un exemple de demande GET pour recevoir la charge utile JSON de données pour la table Incident [incident] :

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Si l'utilisateur accorde l'accès, le jeton est inclus dans l'URL de redirection (rappel) :

```
https/http://{callbackURL}?access_token={the_token}
```

Informations d'identification du client

Utilisez le type d'accord d'informations d'identification du client OAuth pour les intégrations entrantes d'un client OAuth tiers vers la ServiceNow® plateforme.

Les administrateurs peuvent utiliser le type d'accord Informations d'identification du client (CC) pour permettre l'intégration d'un client OAuth tiers à la ServiceNow plateforme.

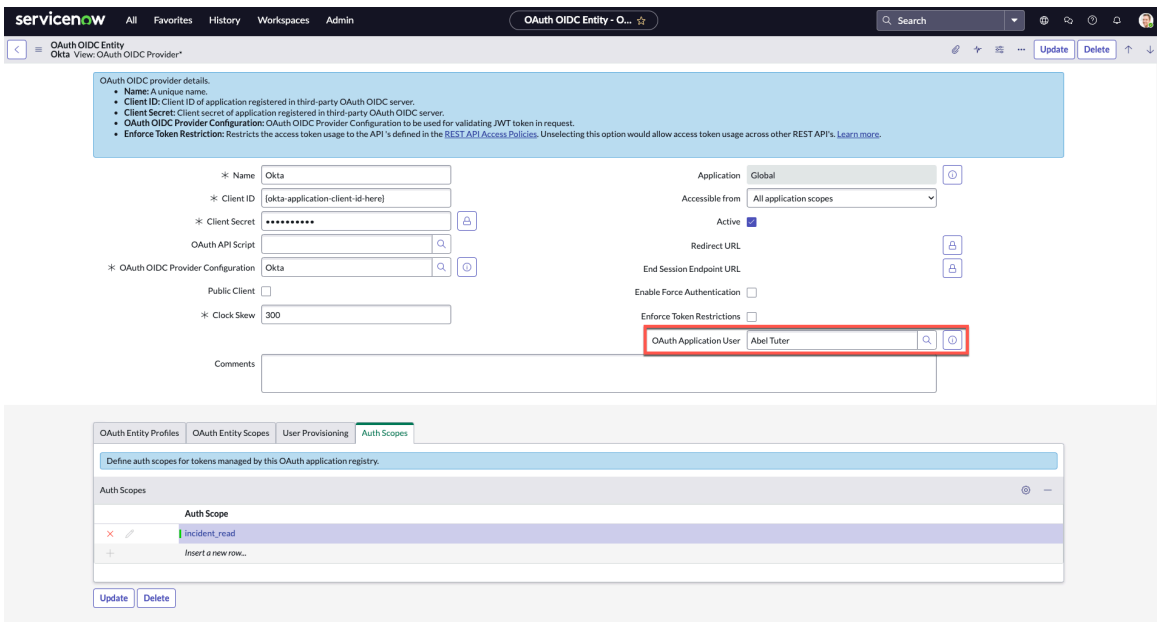
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le type d'attribution d'informations d'identification du client entrant est une aptitude qui peut être contrôlée par le biais d'une propriété système. Par défaut, la propriété système est false.

Pour utiliser le type d'accord Informations d'identification du client, procédez comme suit :

- Créez la propriété système `glide.oauth.inbound.client.credential.grant_type.enabled` .
- Ajoutez le champ **Utilisateur de l'application OAuth** au formulaire Entité OAuth.



Créer la propriété système Informations d'identification du client

Créez la propriété système `glide.oauth.inbound.client.credential.grant_type.enabled` pour utiliser le type d'accord Informations d'identification du client pour les intégrations entrantes OAuth.

Avant de commencer

Rôle requis : admin

Module d'extension requis : OAuth 2.0.

Procédure

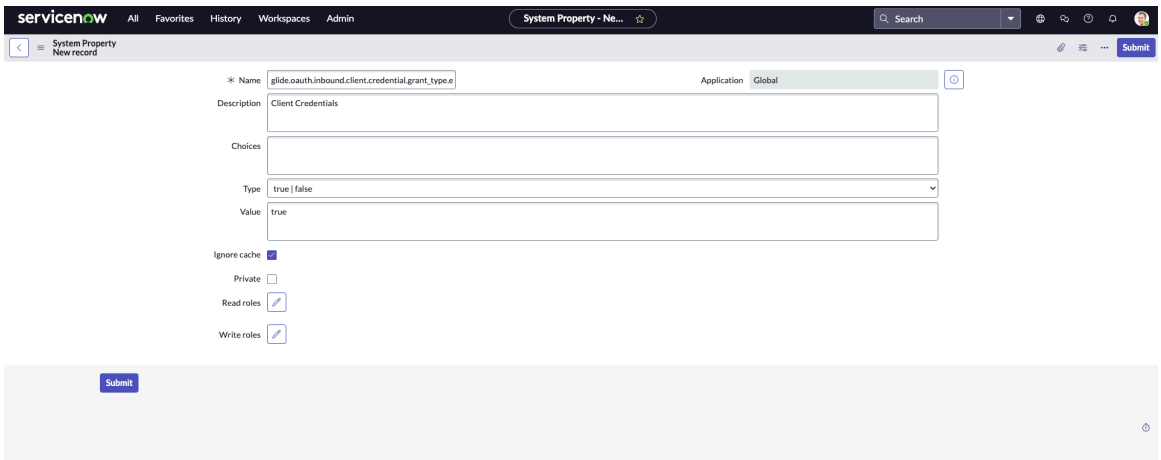
1. Dans le filtre de navigation, saisissez `sys_properties.list`.
   La liste exhaustive des propriétés de la table Propriétés système [sys_properties] s'affiche.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire.

Champ	Description
Nom	Nom de la propriété que vous créez. Dans ce cas, `glide.oauth.inbound.client.credential.grant_type.enabled`.
Description	Saisissez une phrase brève et descriptive décrivant la fonction de la propriété.
Type	Sélectionnez le type de données approprié dans la liste. Dans ce cas, `vrai| faux`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Valeur	Définissez la valeur souhaitée pour la propriété. Dans ce cas, `vrai` pour activer le type d'accord d'informations d'identification du client pour les intégrations entrantes OAuth.



Remarque :
D'autres champs du formulaire, tels que Choix, Ignorer le cache, Privé, Les rôles de lecture et les rôles d'écriture peuvent être configurés en fonction de vos besoins.

4. Sélectionnez **Soumettre**.

Remarque :
Si la case **Ignorer le cache** est cochée, le système vide le cache du serveur lorsque le paramètre est modifié.

Vous devez ensuite créer un client OAuth (point de terminaison d'API OAuth pour le client externe) et ajouter le champ Utilisateur de l'application OAuth à l'enregistrement client OAuth.

Ajouter l'utilisateur de l'application OAuth

Ajoutez le champ Utilisateur de l'application OAuth sur le formulaire Entité OAuth pour utiliser le type d'accord Informations d'identification du client pour les intégrations entrantes OAuth.

Avant de commencer
Rôle requis : admin

Module d'extension requis : OAuth 2.0.

Vous devez créer un client OAuth. Pour plus d'informations, consultez Créer un point de terminaison pour permettre aux clients d'accéder à l'instance.

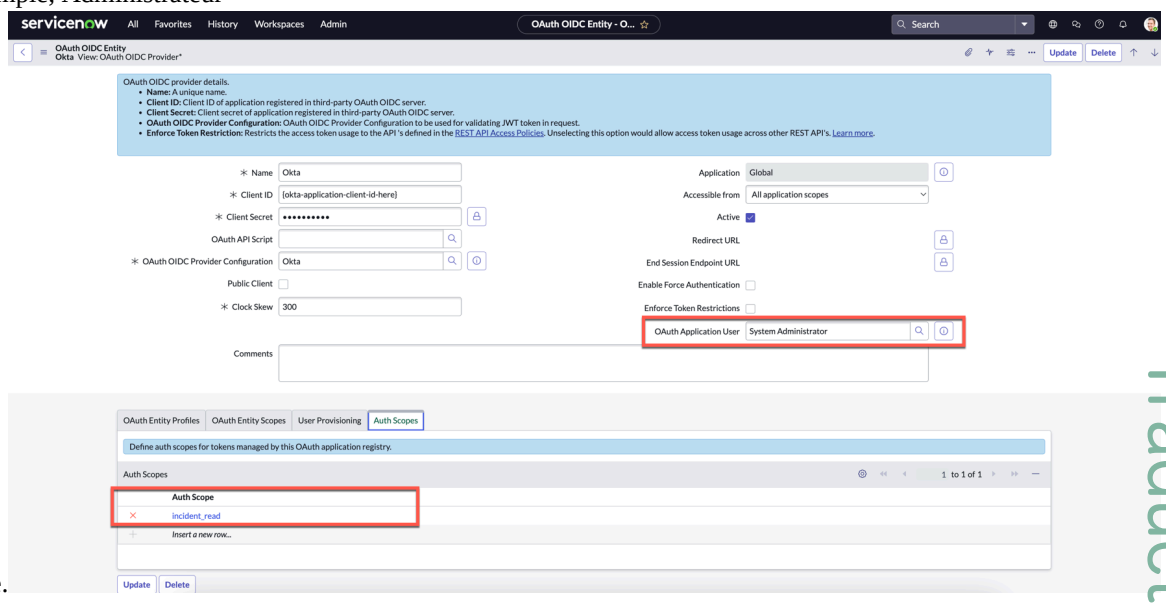
Procédure

1. Ouvrez l'enregistrement client OAuth qui a été créé.
2. Sélectionnez l'icône Plus d'options dans l'en-tête de page.
3. Sélectionner **Configurer** > **Conception de formulaire**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sur la page Conception de formulaire, ajoutez **Utilisateur de l'application OAuth** dans la liste des champs.
5. Enregistrez ou mettez à jour le formulaire.
6. Sélectionnez l'utilisateur pour **l'utilisateur de l'application OAuth**.
   Par exemple, Administrateur système.



> **Remarque :**
> Vous devez utiliser le périmètre d'authentification de l'API REST avec le type d'accord Informations d'identification du client pour contrôler l'accès fourni au client tiers.

7. Enregistrez ou mettez à jour le formulaire.

Toute demande d'autorisation avec le **type d'accord** comme **Informations d'identification du client**, **ID client** et **Secret** est transmise pour l'utilisateur de l'application OAuth associé dans ServiceNow®.

> **Remarque :**
> Si l'utilisateur de l'application OAuth n'est pas sélectionné dans l'enregistrement client OAuth ou si la propriété Informations d'identification du client est définie sur faux, la demande d'autorisation n'est pas transmise.

Gérer les jetons OAuth

Ouvrez les jetons OAuth pour fournir l'accès à des ressources restreintes.

Avant de commencer

Rôle requis : n'importe quel utilisateur ou administrateur

Pourquoi et quand exécuter cette tâche

Les jetons OAuth émis par l'instance et le fournisseur OAuth tiers sont stockés dans oauth_credential table.

Voici quelques-unes des colonnes importantes de ce tableau :

- Jeton : valeur du jeton émis par ServiceNow l'instance.
- Type : détermine si le jeton est un jeton d'accès ou un jeton d'actualisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Date d'expiration : données/heure auxquelles le jeton d'accès ou d'actualisation expire.
- Jeton reçu : valeur du jeton émis par un fournisseur OAuth tiers. Cette valeur est au format chiffré.

L'expiration et la validité du jeton sont les suivantes :

- Jeton d'accès : par défaut, une instance émet des jetons d'accès d'une durée de vie de 30 minutes dans le scénario où l'instance est le fournisseur OAuth.
- Jeton d'actualisation : par défaut, une instance émet des jetons d'actualisation avec une durée de vie de 100 jours dans le scénario où l'instance est le fournisseur OAuth.

Procédure

1. Accédez à l'une des options de menu suivantes :
   - **Libre-service** > **Mes applications connectées** pour voir les jetons créés par l'instance lorsque vous avez accordé l'accès à une ressource sur l'instance.
   - **OAuth système** > **Gérer les jetons** pour voir tous les jetons. Seuls les administrateurs peuvent accéder à ce module.
2. Cliquez sur le **nom** pour ouvrir le jeton.
3. Cliquez sur **Révoquer l'accès** pour empêcher l'accès à la ressource restreinte.

   Vous pouvez également afficher d'autres informations sur le jeton, notamment le périmètre auquel il autorise l'accès et la date d'expiration.

   Vous pouvez sélectionner l'enregistrement **Nettoyer les informations d'identification OAuth expirées** à partir de la page Calendrier (sys.trigger.list) et configurer les éléments suivants :

   - **com.snc.platform.security.oauth.is.active** : par défaut, la valeur est définie sur vrai.
   - **com.snc.platform.security.oauth.hours.expired.credential.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre d'heures pendant lesquelles vous souhaitez conserver les informations d'identification OAuth expirées dans le système.
   - **com.snc.platform.security.oauth.day.old.credential.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver les informations d'identification OAuth expirées dans le système.

Révoquer un jeton OAuth

Il est possible que vous souhaitiez révoquer un accès OAuth ou actualiser le jeton pour des raisons de sécurité.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La révocation du jeton se rapporte à la situation où votre instance agit en tant que serveur de ressources OAuth. Vous pouvez révoquer le jeton via une URL.

Procédure

Accédez à votre instance à l'aide de oauth_revoke_token.do et ajoutez le jeton d'accès ou d'actualisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple : https://[Your_ServiceNow_Instance] :[port]/oauth_revoke_token.do ?token=[jeton d'accès ou d'actualisation] sans les crochets [ ].

Résultats
Cet accès au point de terminaison ne nécessite pas d'authentification. Le jeton de cette demande est marqué comme expiré.

Sortant OAuth

La sortie OAuth vous permet d'extraire des données d'un fournisseur tiers vers votre instance.

Vous devez disposer du rôle security_admin pour gérer l'intégration OAuth.

Vous pouvez configurer OAuth 2.0 sortant pour les types d'accord suivants :

- **Se connecter à un fournisseur tiers** : utilisez l'ID et le secret client pour l'envoyer au fournisseur OAuth. Pour plus d'informations, consultez Se connecter à un fournisseur OAuth tiers.
- **Support JWT** : un serveur d'autorisation valide un jeton JWT qui permet de partager des informations d'identité et de sécurité entre les domaines de sécurité. Pour plus d'informations, consultez Configurer le fournisseur OAuth avec le type d'attribution JWT Bearer.
- **Support SAML2** : génère l'assertion SAML2, puis échange l'assertion contre les jetons d'accès auprès du fournisseur.

  Remarque :
  Pour la demande sortante d'utilisation SuccessFactors du **porteur SAML2** comme type d'octroi par défaut. Pour en savoir plus sur la configuration du **support SAML2**, reportez-vous à l'exemple dans Set up the v4.x.x .

- **Code d'autorisation** : code accordé au client pour obtenir un jeton d'accès, qui est ensuite utilisé pour obtenir l'accès à la ressource. Si vous sélectionnez cette option, vous avez besoin d'une URL d'autorisation (l'URL du serveur d'autorisation).
- **Informations d'identification du mot de passe du propriétaire de ressource** : nom d'utilisateur et mot de passe de l'utilisateur qui essaie d'obtenir l'accès à la ressource.
- **Informations d'identification du client** : ID et secret client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation.
- **Serveur MID** : les serveurs MID facilitent la communication et le déplacement de données entre une instance unique ServiceNow® et des applications, sources de données et services externes. Utilisez les types OAuth du code d'autorisation, des informations d'identification du mot de passe du propriétaire de ressource, du titulaire SAML et du titulaire JWT OAuth pour les demandes d'intégration sortantes via le serveur MID. L'authentification personnelle est également prise en charge via le serveur MID.

Vous pouvez configurer **le scénario du fournisseur OAuth** (sortant) : votre instance extrait les données d'un fournisseur tiers.

Remarque :
Vous devez vous authentifier pour la première fois pour récupérer la publication du jeton, ce que vous n'avez pas besoin d'authentifier à l'aide d'un compte utilisateur avant l'expiration du jeton.

Se connecter à un fournisseur OAuth tiers

Configurez la façon dont l'ID client et la clé secrète sont envoyés à votre fournisseur OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis remplissez le formulaire.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	L'ID client de l'application enregistrée dans le serveur OAuth tiers.
Secret client	Clé secrète du client de l'application enregistrée sur le serveur OAuth tiers.
Script de l'API OAuth	Script utilisé pour personnaliser la demande et la réponse au fournisseur OAuth externe.
URL du logo	L'URL du logo de l'application OAuth.
Type d'accord par défaut	Le type d'accord par défaut utilisé pour établir le jeton. Les choix sont les suivants : ○ **Code d'autorisation** : code accordé au client pour obtenir un jeton d'accès, qui est ensuite utilisé pour obtenir l'accès à la ressource. Si vous sélectionnez cette option, vous avez besoin d'une URL d'autorisation (l'URL du serveur d'autorisation). ○ **Informations d'identification du mot de passe du propriétaire de ressource** : nom d'utilisateur et mot de passe de l'utilisateur qui essaie d'obtenir l'accès à la ressource. ○ **Informations d'identification du client** : ID et secret client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation. ○ **Support JWT** : un serveur d'autorisation valide un jeton JWT qui permet de partager des informations d'identité et de sécurité entre les domaines de sécurité. ○ **Support SAML2** : génère l'assertion SAML2, puis échange l'assertion contre les jetons d'accès auprès du fournisseur. **Remarque :** Pour la demande sortante d'utilisation SuccessFactors du **porteur SAML2** comme type d'octroi par défaut.
Durée de vie du jeton d'actualisation	Durée de validité du jeton d'actualisation, en secondes. La durée par défaut est de 8 640 000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation. **Remarque :** Vous pouvez utiliser uniquement le code d'autorisation `Default Grant type` lorsque PKCE est activé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Méthode de contestation de code	Méthode de contestation de code utilisée dans le workflow PCKE OAuth. Les choix sont les suivants : ○ S256 [Par défaut] ○ Brut ○ Aucun
Commentaires	Ajoutez des commentaires concernant l'application OAuth.
Application	Application et périmètre qui contiennent cet enregistrement.
Accessible depuis	Rendez cette application accessible à partir de tous les périmètres de l'application ou uniquement à partir de ce périmètre.
Actif	Cochez la case pour activer l'application.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Le point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si ce champ est vide, l'instance génère automatiquement une entrée.
Activer l'authentification réciproque	Cochez la case pour utiliser l'authentification réciproque pour la demande et la révocation de jeton. Cette fonctionnalité nécessite la spécification d'un profil d'authentification réciproque.
Envoyer les informations d'identification	Le client OAuth renseigne les informations d'identification du client dans la demande : ○ Dans le corps de la demande (codage URL de formulaire) ○ En-tête d'autorisation de base ○ En tant que clé privée JWT
Type de client	Choisissez le type de client, en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

3. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Profils des entités OAuth pour valider un profil par défaut généré par le système pour le nouveau fournisseur OAuth sans aucun champ d'application.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth comprenant le nom, le type d'accord et le périmètre OAuth.
4. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Périmètres des entités OAuth pour définir tous les champs d'application OAuth disponibles pour ce fournisseur OAuth.
   Vous pouvez sélectionner les champs d'application lorsque vous créez ou mettez à jour un profil. Chaque périmètre OAuth contient un nom et un périmètre que vous devez obtenir à partir de la spécification du fournisseur, telle qu'un périmètre de lecture ou un périmètre d'écriture. Chaque périmètre doit être défini séparément.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Support JWT

Les jetons Web JSON (JWT) permettent de configurer les interactions d'API de serveur à serveur entre ServiceNow les fournisseurs d'API externes sans nécessiter aucune intervention de l'utilisateur.

L'attribution de porteur de jeton Web JSON (JWT) est une chaîne JSON qui contient des valeurs de réclamation qui sont évaluées et validées par les gestionnaires d'octroi JWT du côté du serveur d'autorisation, avant d'émettre un jeton d'accès.

À l'aide du type d'attribution titulaire JWT, vous pouvez configurer le flux d'attribution titulaire JWT OAuth 2.0 pour le message REST sortant.

Configurer le fournisseur OAuth avec le type d'attribution JWT Bearer

Les jetons Web JSON (JWT) permettent de configurer les interactions d'API de serveur à serveur entre ServiceNow les fournisseurs d'API externes sans nécessiter aucune intervention de l'utilisateur. Cette prise en charge active Centre d'intégration ou d'autres tâches automatisées utilisant des JWT pour configurer des intégrations d'API et de services avec différents fournisseurs.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Les tâches suivantes montrent comment ServiceNow configurer l'utilisation de JWT pour les autorisations d'authentification et d'authentification client OAuth 2.0. ServiceNow est le client OAuth et vous pouvez configurer un fournisseur OAuth, tel que Box ou Docusign.

Procédure

1. Télécharger le certificat de magasin de clés Java
   Joignez un certificat JKS à votre instance pour activer l'authentification du client JWT.
2. Configurer une clé de signature JWT
   Créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).
3. Créer un fournisseur JWT avec une clé de signature JWT
   Ajoutez un fournisseur JWT à votre ServiceNow instance.
4. Se connecter à un fournisseur OAuth tiers
   Créez un fournisseur OAuth tiers avec un porteur JWT comme type d'attribution par défaut dans le ServiceNow registre d'application.
5. Spécifier un profil OAuth
   Ouvrez le profil d'entité OAuth du fournisseur OAuth et affectez un fournisseur JWT.

Télécharger le certificat de magasin de clés Java

Vous pouvez joindre un certificat Java KeyStore (JKS) à votre instance pour l'utiliser pour activer l'authentification du client JWT.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Certificat x509**.
2. Remplissez le formulaire selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Nom	Nom unique pour votre certificat.
Notification à l'expiration	Désignez la personne à notifier lorsque le certificat expire.
Avertissement avant l'expiration (en jours)	Envoyez une notification par e-mail à votre gestionnaire de certificats avant l'expiration de votre certificat.
Actif	Permet l'utilisation du certificat pour les demandes de jetons.
Type	Type de certificat que vous chargez.
Échéance en jours	Nombre de jours jusqu'à l'expiration du certificat.
Mot de passe de magasin de clés	Mot de passe associé au certificat.
Description brève	

3. Cliquez sur **Envoyer**.

Configurer une clé de signature JWT

Créez une clé de signature JSON Web Token (JWT) à affecter à votre certificat Java KeyStore (JKS),

Avant de commencer

Rôle requis : admin

Remarque :
Si vous souhaitez ajouter **l'int d'empreinte SHA-1 du certificat X.509 (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d'empreinte **SHA-1 du certificat X.509 (x5t).**

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Clés JWT**.
2. Remplissez le formulaire selon vos besoins.

Option	Description
Nom	Nom unique pour votre configuration de signature de clé JWT.
Magasin de clés de signature	Le magasin de clés désigné lors de la signature de JWT.
ID clé	L'ID de clé (enfant) permet d'identifier la clé utilisée lorsque plusieurs clés sont utilisées pour signer des jetons.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Si vous configurez ce champ, la réclamation d'ID de clé est incluse dans JWT. Si vous ne configurez pas ce champ, votre JWT n'aura pas de réclamation d'ID de clé.
Algorithme de signature	L'algorithme à utiliser pour signer avec la clé JWT. RSA 256 est le seul algorithme disponible.
Signature avec le mot de passe de clé	Mot de passe associé à la clé de signature.
Actif	Indiquez que l'alias de clé JWT est activement référencé à partir d'un fournisseur JWT.

3. Cliquez sur **Envoyer**.

Créer un fournisseur JWT avec une clé de signature JWT

Ajoutez un fournisseur de jeton Web JSON (JWT) à votre ServiceNow instance.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Fournisseur JWT**.
2. Remplissez le formulaire et cliquez sur **Soumettre**.

Option	Description
Nom	Nom unique pour la configuration de votre fournisseur JWT.
Intervalle d'expiration (s)	La durée de vie des jetons, en secondes, générés par le fournisseur JWT.
Configuration de la signature	La ServiceNow configuration de clé de signature JWT à appliquer.

Générer un jeton Web JSON (JWT)

Créez un jeton Web JSON (JWT) pour représenter les réclamations en toute sécurité entre deux parties sur le .ServiceNow AI Platform

L'API GlideJWT est une API scriptable et incluse dans le périmètre qui génère un JWT. Trois arguments sont nécessaires avant de générer le JWT :

- Sys_id du fournisseur JWT
- En-tête sérialisé JSON
- Charge utile sérialisée JSON

Il existe deux scripts d'API JWT, JWTTokenInternal et JWTTokenRestricted, que vous pouvez utiliser lors de la configuration d'un fournisseur JWT. Le script JWTTokenRestricted permet aux administrateurs de configurer qui peut générer un JWT. Le script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

JWTTokenInternal est en lecture seule et permet uniquement aux utilisateurs connectés de générer un JWT.

Pour générer un JWT :

- Créer une clé JWT avec une clé partagée (HMAC) ou un magasin de clés de signature (RSA)
- Associer un fournisseur JWT à la configuration de signature faisant référence à une clé JWT

Vous pouvez utiliser l'API pour créer votre jeton.

Vous pouvez utiliser des réclamations standard et personnalisées lors de la configuration d'un fournisseur JWT. Vous pouvez transmettre des réclamations d'en-tête dynamique et de charge utile dans le cadre de la signature de l'API generateJWT.

Exemple de script pour tester l'API :

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub": "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

API clientes OAuth

L'API cliente OAuth fournit des méthodes permettant de demander et de révoquer les jetons OAuth.

Le client OAuth fournit les classes suivantes :

- GlideOAuthClient : méthodes de demande et de révocation des jetons d'actualisation et d'accès.
- GlideOAuthClientRequest : méthodes de traitement des demandes des clients.
- GlideOAuthClientResponse : méthodes de gestion des réponses des clients.
- GlideOAuthToken : méthodes de récupération du jeton d'accès et des informations relatives au jeton d'accès.

Vous pouvez également personnaliser l'include de script OAuthUtil pour intercepter les paramètres de demande et analyser les réponses des fournisseurs OAuth externes.

Lors de l'utilisation des classes OAuth dans un script inclus dans le périmètre, utilisez l'identificateur de l'espace de noms `sn_auth` .

Paramètres OAuth pour la prise en charge des profils par défaut

La fonctionnalité de profil par défaut nécessite un ensemble de paramètres que vous pouvez utiliser avec l'API *`setParameter()`* pour spécifier le demandeur OAuth, un contexte pour la demande et le profil du fournisseur.

Dans le scénario du fournisseur OAuth, vous devez définir trois paramètres qui indiquent au fournisseur OAuth le profil OAuth à utiliser par défaut. Lorsque ces trois paramètres sont définis, le jeton d'accès est enregistré dans la base de données de l'instance. Utilisez les paramètres avec *`GlideOAuthClientRequest`*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres OAuth pour la prise en charge des profils par défaut

Paramètre	Description
oauth_requestor	Le sys_id de l'objet, qui peut être un enregistrement utilisateur ou un compte de messagerie.
oauth_requestor_context	Descripteur qui fournit un contexte au demandeur OAuth. En bonne pratique, utilisez le nom de la table dans laquelle l'objet oauth_requestor est enregistré.
oauth_provider_profile	sys_id de l'enregistrement de profil OAuth par défaut (voir Spécifier un profil OAuth).

Vous n'avez pas besoin d'utiliser de paramètres pour définir le type d'octroi et le champ d'application, car les valeurs sont configurées dans l'enregistrement de profil OAuth. Si vous n'utilisez pas les paramètres, vous pouvez utiliser les méthodes d'API GlideOAuthClientRequest *setScope* et *setGrantType*. Pour plus d'informations, consultez setScope et setGrantType .

Clé privée Prise en charge de JWT pour l'authentification client OAuth 2.0

Prise en charge JWT Prise en charge de l'authentification client OAuth 2.0.

Clé privée L'authentification client JWT est une méthode d'authentification qui peut être utilisée par les clients pour s'authentifier auprès du serveur d'autorisation lors de l'utilisation du point de terminaison de jeton.

Dans ce mécanisme d'authentification, seuls les clients qui ont enregistré une clé publique et signé un JWT à l'aide de cette clé peuvent s'authentifier.

Le JWT doit contenir des valeurs de réclamation REQUISES et peut contenir des valeurs de réclamation FACULTATIVES. Pour en savoir plus sur les valeurs de réclamation nécessaires pour le JWT pour l'authentification private_key_jwt , reportez-vous à la section Authentification du client dans la documentation de base d'OpenID Connect .

Remarque :
Le jeton d'authentification doit être envoyé comme la valeur du paramètre client_assertion. La valeur du paramètre **client_assertion_type** doit être urn :ietf :params :oauth :client-assertion-type :jwt-bearer.

Modules d'extension requis pour l'authentification client OAuth 2.0 à l'aide d'un jeton JWT :

- **OAuth 2.0 (com.snc.platform.security.oauth)** : ce module d'extension est actif sur les instances nouvelles et mises à niveau. Si le module d'extension n'est pas actif sur votre instance, vous pouvez l'activer.
- **Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer)** : pour le cas d'utilisation de l'authentification unique basée sur OIDC.

Vous pouvez utiliser l'authentification client OAuth 2.0 à l'aide de Private Key JWT pour les éléments suivants :

- Authentification unique basée sur OIDC
- Intégrations OAuth sortantes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la clé privée JWT pour l'authentification SSO basée sur OIDC

Configurez le JWT de clé privée pour les intégrations SSO basées sur OIDC.

Avant de commencer

Rôle requis : admin

Vous devez effectuer les tâches suivantes avant de choisir Clé privée JWT pour le SSO basé sur OIDC.

- Télécharger le certificat de magasin de clés Java: joignez un certificat JKS à votre instance pour activer l'authentification du client JWT.
- Configurer une clé de signature JWT: créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).

> **Remarque :**
> Si vous souhaitez ajouter **l'int d'empreinte SHA-1 du certificat X.509 (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d'empreinte **SHA-1 du certificat X.509 (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajouter un fournisseur JWT à votre ServiceNow instance.

Pour inclure une clé JWT pour le fournisseur d'identité basé sur OIDC, vous devez :

- Installez le module d'extension **Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** (com.snc.integration.sso.multi.installer).
- Activez les propriétés pour les **propriétés SSO de plusieurs fournisseurs**. Pour plus d'informations, consultez Propriétés, tables et scripts SSO de plusieurs fournisseurs.
- Créez un fournisseur d'identité OIDC. Pour plus d'informations, consultez Créer une configuration OpenID Connect (OIDC) pour l'authentification unique (SSO).

Procédure

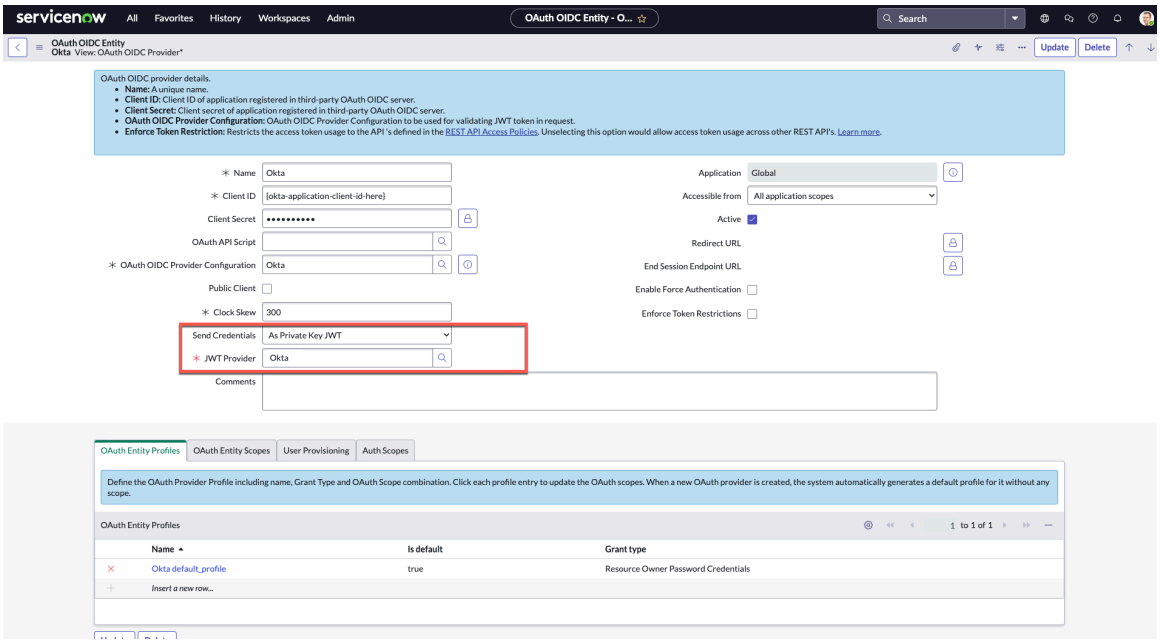
1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
2. Sélectionnez le fournisseur d'identité OIDC que vous avez créé.
3. En haut du formulaire, sélectionnez **Configurer** > **Conception de formulaire**.

> **Remarque :**
> Vous devez ajouter les champs **Envoyer les informations d'identification** et **Fournisseur JWT** au formulaire pour utiliser la clé privée JWT pour les demandes d'authentification du fournisseur d'identité basées sur OIDC.

4. Choisissez Comme **clé privée JWT** pour envoyer les informations d'identification.
5. Sélectionnez le **fournisseur JWT**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque l'utilisateur s'authentifie, la page d'authentification dispose d'options pour se connecter via Okta.

Configurer la clé privée JWT pour OAuth sortant

Configurez la clé privée JWT pour les intégrations OAuth sortantes.

Avant de commencer

Rôle requis : admin

Avant de configurer le JWT de clé privée pour les intégrations OAuth sortantes, vous devez effectuer les tâches suivantes :

- Télécharger le certificat de magasin de clés Java: joignez un certificat JKS à votre instance pour activer l'authentification du client JWT.
- Configurer une clé de signature JWT: créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).

> **Remarque :**
> Si vous souhaitez ajouter **l'int d'empreinte SHA-1 du certificat X.509 (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d'empreinte **SHA-1 du certificat X.509 (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajouter un fournisseur JWT à votre ServiceNow instance.

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis remplissez le formulaire.

> **Remarque :**
> Vous devez ajouter les champs **Envoyer les informations d'identification** et **Fournisseur JWT** au formulaire pour utiliser la clé privée JWT pour les demandes d'authentification OAuth sortantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	L'ID client de l'application enregistré sur le serveur OAuth tiers.
Secret client	Clé secrète du client de l'application enregistrée sur le serveur OAuth tiers.
Script de l'API OAuth	Script utilisé pour personnaliser les demandes et les réponses au fournisseur OAuth externe.
URL du logo	L'URL du logo de l'application OAuth.
Type d'accord par défaut	Choisissez : **Informations d'identification du client** : l'ID client et le secret client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation.
Durée de vie du jeton d'actualisation	Durée de validité du jeton d'actualisation, en secondes. La durée par défaut est de 8 640 000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation. **Remarque :** Vous pouvez utiliser uniquement le code d'autorisation `Default Grant type` lorsque PKCE est activé.
Commentaires	Ajoutez des commentaires concernant l'application OAuth.
Application	Application et périmètre qui contiennent cet enregistrement.
Accessible depuis	Rendez cette application accessible à partir de tous les périmètres de l'application ou uniquement à partir de ce périmètre.
Actif	Cochez la case pour activer l'application.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Le point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si ce champ est vide, l'instance génère automatiquement une entrée.
Activer l'authentification réciproque	Cochez la case pour utiliser l'authentification réciproque pour la demande et la révocation de jeton. Cette fonctionnalité nécessite la spécification d'un profil d'authentification réciproque.
Envoyer les informations d'identification	Choisir : **En tant que clé privée JWT**
Fournisseur JWT	Détails du fournisseur JWT. Vous pouvez utiliser la recherche pour sélectionner le fournisseur JWT.

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type Fournisseur OAuth qui peut être utilisé pour l'authentification par clé JWT privée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un message REST sortant

Créez un message REST sortant pour autoriser l'instance en tant que serveur d'autorisation.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Services web du système** > **Sortant** > **Message REST** , puis cliquez sur **Nouveau**.
2. Renseignez les champs de formulaire de l'enregistrement d'application OAuth comme décrit dans .
   Notez les valeurs de champ suivantes :
   - **Point de terminaison** : URL de l'instance qui constitue le serveur d'autorisation.
   - **Type d'authentification** : **OAuth 2.0**.
   - **Profil OAuth** : profil OAuth que vous avez créé pour le serveur client.
3. Dans l'enregistrement du message REST, cliquez sur **Obtenir un jeton OAuth**.
4. Authentifiez-vous auprès de l'instance qui fournit le jeton : la méthode dépend de l'intégration de l'authentification unique.
   Vous pouvez utiliser :
   - Nom d'utilisateur et mot de passe que vous utilisez pour vous authentifier sur l'instance.
   - Le nom d'utilisateur et le mot de passe de l'IdP si est activé. Cliquez sur **Utiliser une connexion externe** pour accéder à l'écran de connexion IdP.

     Remarque :
     Pour être automatiquement redirigé vers la page de connexion IdP, vous devez définir la propriété système glide.authenticate.external.

   - Votre code, si la MFA est activée.
5. Cliquez sur **Autoriser** ou **Refuser** pour terminer l'autorisation et émettre les jetons.
   Le processus qui suit est décrit dans la section Flux d'octroi du code d'autorisation OAuth.

Authentification personnelle

L'authentification personnelle vous permet de vous connecter et de gérer en toute sécurité vos intégrations basées sur OAuth telles que Microsoft OneDrive ou Google Drive.

Informations d'identification OAuth 2.0

Le module Informations d'identification OAuth 2.0 dans ServiceNow (oauth_2_0_credentials) vous permet de configurer et de gérer les jetons d'accès utilisés pour vous connecter à des systèmes externes compatibles OAuth 2.0. Utilisez le type d'intégration Personnel lorsque chaque utilisateur doit s'authentifier avec sa propre identité auprès d'un système externe.

Utilisez le formulaire Informations d'identification pour configurer les informations d'identification OAuth 2.0 avec integration_type = Personnel. Pour plus d'informations, consultez Informations d'identification OAuth 2.0.

L'authentification personnelle n'est prise en charge que pour les types d'accords OAuth 2.0 suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Code d'autorisation
- Informations d'identification du mot de passe du propriétaire de ressource (ROPC)

Les types d'attribution tels que les informations d'identification du client et l'attribution JWT Bearer ne sont pas pris en charge avec integration_type = Personnel.

Remarque :
L'authentification personnelle est également prise en charge via un serveur MID pour les types de code d'autorisation et d'attribution ROPC. Pour plus d'informations, consultez Extraction du jeton OAuth via MID.

Tableau de bord d'authentification personnelle

Utilisez vos informations d'identification personnelles pour vous connecter à des intégrations tierces. Affichez, authentifiez, révoquez et renouvelez vos authentifications personnelles via une interface simplifiée et consolidée. Pour plus d'informations, consultez Using the Personal Authentication dashboard .

Remarque :
Le tableau de bord d'authentification personnelle n'est accessible qu'aux utilisateurs affectés au rôle : sn_personal_auth.personal_auth_user

Configurer l'authentification personnelle

Vous pouvez configurer l'authentification OAuth personnelle avec l'étape REST dans Concepteur de flux.

Avant de commencer
Rôle requis : admin

Assurez-vous d'installer le programme d'installation du pack de démarrage Centre d'intégration (com.glide.hub.integrations) ou une version supérieure.

Pourquoi et quand exécuter cette tâche
Cette tâche vous guide dans la configuration de l'authentification OAuth personnelle pour les étapes REST dans ServiceNow® Concepteur de flux. Il permet l'exécution des appels REST à l'aide des informations d'identification de l'utilisateur de session, garantissant un accès sécurisé et personnalisé à l'API.

Pour en savoir plus sur la vérification de l'existence d'un jeton OAuth personnel pour un utilisateur, reportez-vous à la section Obtenir un jeton OAuth personnel (à l'aide de GlideOAuthClient).

Pour en savoir plus sur la génération du jeton initial pour un utilisateur qui n'a pas accès à la page des informations d'identification, reportez-vous à la rubrique Générer l'URL de l'initiateur d'authentification personnelle.

Procédure

1. Accédez aux **registres d'application** et créez un registre d'application OAuth pour vous connecter à un point de terminaison externe.
2. Accédez aux **alias de connexion et d'informations d'identification**, puis créez un alias de connexion. Cet alias est utilisé dans les étapes REST. Pour plus d'informations, consultez Créer un alias de connexion et d'informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Accédez à **la connexion HTTP(s)** et mettez à jour les détails du point de terminaison externe pour l'enregistrement de connexion créé à l'étape précédente.
4. Créez des **informations d'identification OAuth**.
   a. Accédez aux **informations d'identification OAuth 2.0**.
   b. Créez un nouvel enregistrement d'informations d'identification OAuth et liez-le au profil OAuth créé à l'étape 1.
5. Ajoutez le champ **IntegrationType** au formulaire d'informations d'identification.
6. Mettez à jour le champ **IntegrationType** des informations d'identification créées à l'étape 4 sur **Personnel**.
7. Générez un jeton d'accès personnel.
   a. En tant qu'utilisateur connecté, ouvrez l'enregistrement des informations d'identification.
   b. Sélectionnez **Obtenir un jeton OAuth** pour créer un jeton personnel.
   c. Sélectionnez **Gérer les jetons** pour afficher et gérer les jetons.

> **Remarque :**
> Ajoutez une action d'interface utilisateur à votre application afin que les utilisateurs finaux puissent générer des jetons. Seuls les administrateurs peuvent ouvrir directement le formulaire d'informations d'identification.

8. Accédez à **Action** pour créer une action pour votre cas d'utilisation.
9. Ajoutez une étape REST à l'action.
   Sélectionnez l'alias de connexion créé à l'étape 2.

> **Remarque :**
> Testez l'action avec l'appel sortant REST. Les informations d'identification sont marquées pour être utilisées pour l'intégration personnelle. L'étape REST peut afficher une erreur car l'action s'exécute avec le rôle d'intégration système.

10. Créez un nouveau flux secondaire et ajoutez l'action créée à l'étape 8.
    a. Dans la fenêtre **Propriétés du flux secondaire** , sélectionnez **Utilisateur qui lance la session** dans le champ de texte **Exécuter en tant que** .
    Ne sélectionnez pas **Utilisateur système** à la place dans le champ de texte **Exécuter en tant que** .
11. Testez le flux secondaire.
    L'étape REST utilise le jeton créé pour l'utilisateur de la session. Le flux secondaire peut également être appelé à l'aide de FlowAPI.

Exemple de script pour appeler un flux secondaire :

```
try {
   // Execute synchronously in the foreground. Allows access to subflow
 outputs.
   var result = sn_fd.FlowAPI.getRunner()
      .subflow('global.getpersonalincidentssubflow')
      .inForeground()
      .run();

   var outputs = result.getOutputs();
} catch (ex) {
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    var message = ex.getMessage();
    gs.error(message);
}
```

12. Gérez les jetons manquants ou expirés.

    Si l'utilisateur de session n'a pas de jeton d'accès, la demande REST renvoie une réponse **de code d'état HTTP 401 Non autorisé** . Assurez-vous que le jeton est créé avant d'initier le flux.

    Si le jeton d'accès a expiré, mais qu'il existe un jeton d'actualisation valide, le système renouvelle automatiquement le jeton d'accès.

Obtenir un jeton OAuth personnel (à l'aide de GlideOAuthClient)

Vérifiez si l'utilisateur possède un jeton OAuth personnel. Utilisez-la pour confirmer un accès valide avant d'exécuter des étapes REST ou des intégrations qui nécessitent des informations d'identification OAuth personnelles.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Utilisez l'API GlideOAuthClient pour vérifier si un jeton OAuth personnel existe pour l'utilisateur actuellement connecté. Vous pouvez également utiliser ScopedPersonalAuthAPI pour obtenir le jeton OAuth personnel. Pour plus d'informations, consultez PersonalAuthAPI - Scoped .

Procédure

1. Utilisez l'exemple de script suivant pour vérifier l'existence d'un jeton d'accès personnel associé à l'utilisateur de la session en cours :

```
function dumpToken(token) {
  if (token) {
    gs.info("Access token: " + token.getAccessToken());
    gs.info("Expires in: " + token.getExpiresIn());
    gs.info("Refresh token: " + token.getRefreshToken());
  }
}

var oAuthClient = new sn_auth.GlideOAuthClient();
oAuthClient.setPersonal(true); // Returns the token for the logged-in user

var token = oAuthClient.getToken('<credential_sys_id>', '<oauth_profile_sys_id>');
dumpToken(token);
```

2. Remplacez <credential_sys_id> et <oauth_profile_sys_id> par les valeurs d'enregistrement appropriées.
   La méthode setPersonal(true) confirme que le jeton retourné appartient à l'utilisateur actuellement connecté.

Remarque :
Pour plus d'informations sur les méthodes de demande et de révocation des jetons d'actualisation et d'accès OAuth, consultez : Documentation de l'API cliente OAuth Glide .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Générer l'URL de l'initiateur d'authentification personnelle

Générez le jeton initial pour un utilisateur qui n'a pas accès à la page Informations d'identification afin de configurer l'authentification personnelle.

Avant de commencer

Rôle requis : connection_admin

Pourquoi et quand exécuter cette tâche

Les utilisateurs sans le rôle **connection_admin** ne peuvent pas accéder à la page Informations d'identification pour générer des jetons OAuth. Ces utilisateurs doivent générer un jeton personnel à l'aide de l'URL oauth_initiator avec un paramètre supplémentaire indiquant que le jeton est personnel et demandé pour l'utilisateur de la session.

Vous pouvez également utiliser PersonalAuthAPI avec le module d'extension sn_personal_auth pour générer l'URL de l'initiateur. Pour plus d'informations, consultez PersonalAuthAPI : getInitiatorURL(String aliasId)

Remarque :
Si le module d'extension d'authentification personnelle (com.snc.sn_ihub_personal_auth) est activé, utilisez l'API incluse dans le périmètre pour générer l'URL de l'initiateur. Ceci. L'API n'est disponible que si le module d'extension est installé.

Procédure

1. Utilisez le format suivant pour construire l'URL de génération de jeton pour le type d'accord de mot de passe :

```
https://<instance-name>.service-now.com/oauth_password_input.do?
sysparm_oauth_requestor_context=oauth_2_0_credential&sysparm_oauth_requestor=
<credential⌧sys_id>&sysparm_oauth_provider_profile=<OAUTH⌧profile⌧sys_id>&sysparm_oau
th_personal=true
```

2. Utilisez le format suivant pour construire l'URL de génération de jeton pour le type d'accord de code d'autorisation :

```
https:// ://<instance-name>.service-now.com /oauth_initiator.do?
oauth_requestor_context=oauth_2_0_credentials&oauth_requestor=
<credential⌧sys_id>&oauth_provider_profile=<OAUTH⌧profile⌧sys_id>&response_type=code&
personal=true
```

Activer le tableau de bord d'authentification personnelle

Vous pouvez activer le module d'extension Personal Authentication (com.snc.sn_ihub_personal_auth) si Centre d'intégration vous disposez du rôle administrateur. L'application inclut des données de démonstration et installe les applications et modules d'extension connexes ServiceNow® Store , le cas échéant.

Avant de commencer

Centre d'intégration nécessite un abonnement distinct du reste de ServiceNow AI Platform.

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si un module d'extension acheté n'est pas activé automatiquement, vous pouvez l'activer manuellement à partir de la liste Toutes les applications de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Avant d'acheter un abonnement, vous pouvez évaluer la fonctionnalité sur une instance de non-production sans frais en la demandant auprès du Now Support Catalogue de services.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec Centre d'intégration :

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Personal Authentication (com.snc.sn_ihub_personal_auth) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

S'inscrire automatiquement auprès de l'instance ServiceNow

Utilisez l'enregistrement automatique des utilisateurs externes pour intégrer un grand nombre d'utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d'identité pour améliorer l'expérience client et prend en charge les flux d'inscription couramment utilisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’auto-inscription.

Activer



Découvrez comment activer l’auto-enregistrement externe.

Configurer



Configurez l’auto-enregistrement.

Activer



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l’auto-inscription

Utilisez l’enregistrement automatique des utilisateurs externes pour intégrer un grand nombre d’utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d’identité pour améliorer l’expérience client et prend en charge les flux d’inscription couramment utilisés.

L’enregistrement utilisateur externe automatique permet à un grand groupe d’utilisateurs de s’inscrire à une ServiceNow application sans l’aide d’un administrateur. Par exemple, une université avec un grand groupe d’étudiants ayant besoin d’un parking sur le campus pourrait s’inscrire à l’application de stationnement du campus. Chaque étudiant se verrait attribuer un ensemble limité de privilèges spécifiques au stationnement et suivrait un processus d’inscription automatisé. Ce système pourrait générer un numéro de stationnement, unique à chaque étudiant, et s’assurer qu’il avait une place de stationnement.

Un flux d’auto-inscription se compose d’une application personnalisée ServiceNow , dans ce cas, une application de stationnement de campus. Après avoir configuré une application avec les tables nécessaires, un administrateur configure l’inscription, y compris un flux de préinscription, un mappage de champs, un mappage après inscription, un captcha, un mappage de rôle et un flux de post-inscription.

Activer l’enregistrement utilisateur externe automatique

Vous pouvez activer le module d’extension Enregistrement automatique de l’utilisateur externe (com.snc.external_user_self_registration) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d’informations sur les composants installés avec un module d’extension, voir Rechercher les composants installés avec une application .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles externes dans l'auto-inscription

Pour éviter de fournir par inadvertance l'accès à des utilisateurs externes, vous pouvez affecter le rôle de snc_external à tous les utilisateurs externes.

Les utilisateurs externes qui s'auto-inscrivent doivent se voir attribuer le rôle de snc_external, qui compte le moins de privilèges. Le rôle snc_external indique que l'utilisateur est externe à votre organisation et ne doit pas avoir accès aux ressources à moins d'y être explicitement autorisé par les ACL pour le rôle snc_external ou pour des rôles supplémentaires qui héritent du rôle snc_external.

Par défaut, les utilisateurs dotés du rôle snc_external ne peuvent pas accéder aux éléments suivants :

- Tables sans le rôle qui hérite du rôle snc_external ou du rôle public.
- Ressources qui ne sont pas de type Enregistrement, telles que les processeurs et les pages de l'interface utilisateur sans le rôle snc_external ou un rôle qui hérite du rôle snc_external.
- Tableaux de bord Platform Analytics.

À partir de la version Paris, vous devez activer une propriété de liste d'exclusion pour appliquer l'affectation explicite de rôles snc_external. Pour plus d'informations sur l'activation de la propriété, voir Empêcher les affectations futures de rôles internes pour les utilisateurs externes .

Configurer une configuration d'inscription utilisateur pour les utilisateurs externes

Créez un enregistrement de configuration d'inscription de l'utilisateur pour amorcer le processus d'intégration des utilisateurs externes aux applications personnalisées ServiceNow . Ce formulaire guide les utilisateurs externes tout au long du processus d'auto-inscription.

Avant de commencer

- Rôle requis : admin
- Activer l'enregistrement utilisateur externe automatique

Procédure

1. Accédez à la **Tous** > **Enregistrement utilisateur externe automatique** > **Configurations de l'inscription de l'utilisateur** et cliquez sur **Nouveau**.
2. Remplissez les champs du formulaire.

Formulaire de configuration de l'inscription de l'utilisateur

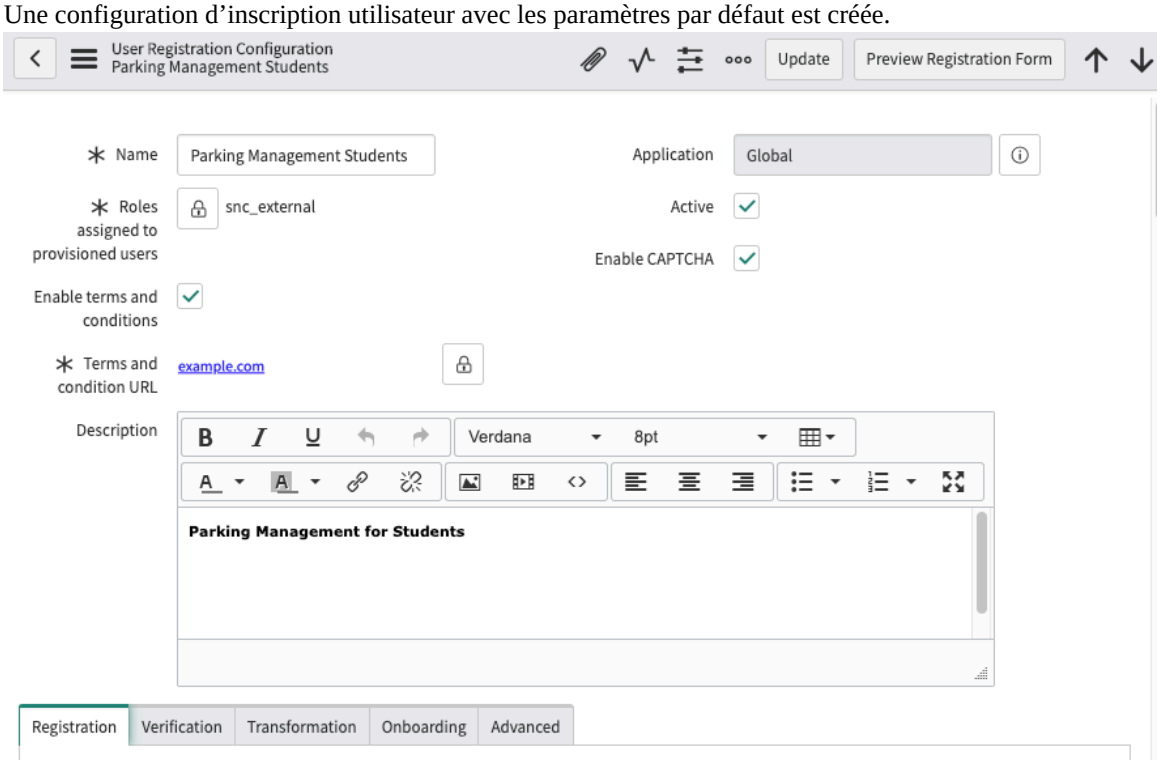
Champ	Description
Nom	Nom du formulaire d'inscription. Par exemple, un étudiant qui s'inscrit au stationnement peut être Étudiants en gestion du stationnement.
Rôles appliqués aux utilisateurs attribués	Rôles affectés aux utilisateurs attribués. Les rôles spécifiés doivent étendre ou contenir le rôle `snc_external` . Le rôle spécifié peut également être `snc_external` rôle. Pour les utilisateurs externes, chaque rôle doit avoir une `snc_external` pour notifier un utilisateur externe. Si vous avez des rôles préconfigurés, les rôles doivent être accessibles lorsque vous déverrouillez les rôles et recherchez des utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Activer les termes et conditions	Option permettant d'ajouter une URL des termes et conditions à la page d'inscription.
URL des termes et conditions	L'URL accessible au public qui contient les termes et conditions du formulaire d'inscription. Ce champ est disponible uniquement lorsque **l'option Activer les termes et conditions** est sélectionnée.
Description	La description du formulaire d'inscription. Ce champ s'affiche uniquement lorsque vous enregistrez ou soumettez la configuration. Vous pouvez ajouter plus d'informations sur le formulaire d'inscription dans ce champ. **Remarque :** Vous ne pouvez ajouter une description qu'après avoir enregistré ou mis à jour une configuration d'inscription utilisateur.
Application	Application contenant cet enregistrement. L'application est automatiquement définie sur Global.
Actif	Option qui active la configuration de l'inscription de l'utilisateur. Cette option est sélectionnée par défaut.
Activer CAPTCHA	Option permettant d'ajouter un CAPTCHA au formulaire d'inscription. Le fournisseur CAPTCHA par défaut est Google reCAPTCHA. **Remarque :** Pour activer CAPTCHA pour l'inscription de l'utilisateur, suivez les étapes de la section Configurer pour l'auto-inscription Google reCAPTCHA de l'utilisateur externe.

3. Cliquez sur **Envoyer**.
Une configuration d'inscription utilisateur avec les paramètres par défaut est créée.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

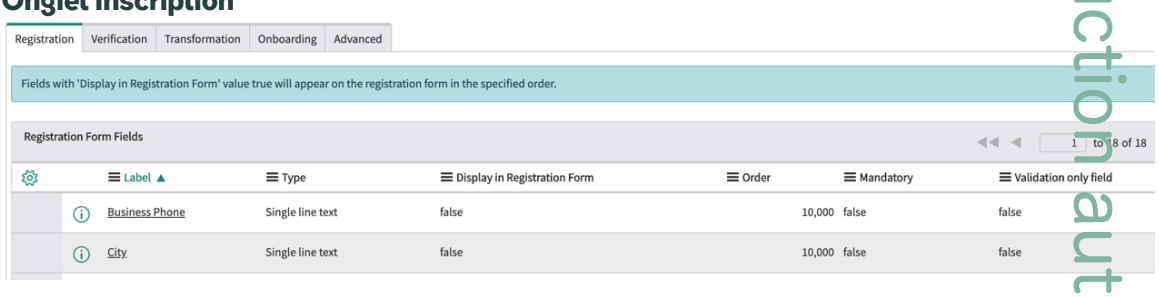
4. **Facultatif :** Configurez l’onglet **Inscription** pour afficher les champs et leur ordre d’affichage :

Champs de formulaire d'inscription

Colonne	Description
Afficher dans le formulaire d'inscription	Définissez tous les champs que vous souhaitez afficher sur Vrai.
Ordre	Définissez un numéro d’ordre pour afficher les champs sur votre formulaire.
Obligatoire	Définissez tous les champs que vous souhaitez rendre obligatoires sur Vrai.
Champ de validation uniquement	Définissez n’importe quel champ que vous voulez utiliser uniquement pour la validation. Par exemple, le code d’inscription.

Vous pouvez choisir d’afficher les champs de formulaire par défaut ou d’ajouter des champs de formulaire personnalisés au formulaire d’inscription. Pour plus d'informations, consultez Champs de formulaire d’inscription par défaut.

Onglet Inscription



Vous pouvez également ajouter des champs de formulaire d’inscription personnalisés. Pour plus d'informations, consultez Ajouter un champ de formulaire d’inscription personnalisé.

5. **Facultatif :** Configurez l'onglet **Vérification** pour vérifier l'identité des utilisateurs enregistrés. Lorsque le flux de vérification de l’utilisateur se déclenche, un lien d’activation est envoyé à l’adresse e-mail enregistrée de l’utilisateur.

Champs de l’onglet Vérification

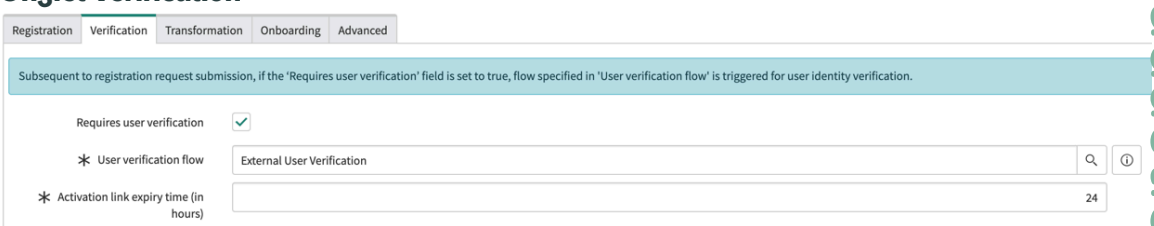
Champ	Description
Requiert une vérification de l'utilisateur	Option permettant de déclencher un flux secondaire de vérification de l’utilisateur qui s’exécute après l’inscription de l’utilisateur. Le flux secondaire est destiné à la vérification de l’identité de l’utilisateur.
Flux de vérification de l'utilisateur	Flux secondaire utilisé pour vérifier l’identité de l’utilisateur. Le flux secondaire se déclenche uniquement lorsque vous activez la vérification de l’utilisateur. (Optional) Le flux secondaire **Vérification de l’utilisateur externe** est disponible par défaut. Vous pouvez créer une copie du flux secondaire par défaut et le Studio

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

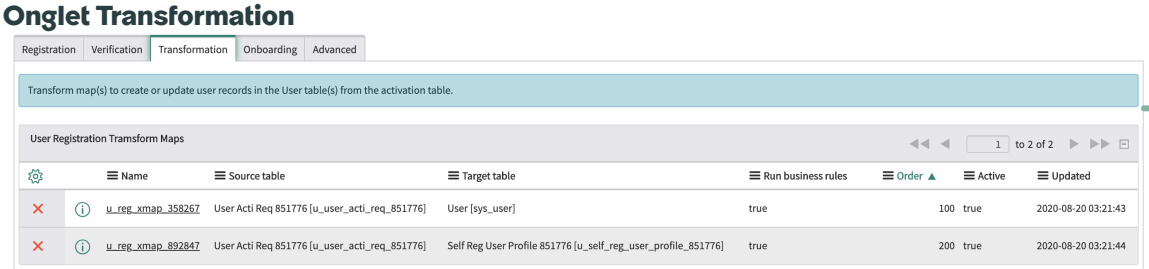
Champ	Description
	de workflow modifier en fonction de vos besoins. Pour en savoir plus, reportez-vous àFlow Designer . **Remarque :** Pour prévisualiser le flux secondaire **Vérification de l'utilisateur externe** dans un nouvel onglet, utilisez les raccourcis suivants : ○ Macintosh : Commande + clic ○ Windows : Ctrl + clic
Délai d'expiration du lien d'activation (en heures)	Nombre d'heures après lesquelles un lien d'activation expire. La valeur par défaut est 24.

Onglet Vérification



6. **Facultatif :** Configurez l'onglet **Transformation** pour mapper les utilisateurs enregistrés automatiquement et les utilisateurs activés.
   Il existe deux cartes de transformation (u_reg_xmap_[numéro]) qui mappent automatiquement les utilisateurs enregistrés de la table Demande d'action d'utilisateur [numéro] à la table Utilisateur enregistré automatiquement [nombre]. Vous pouvez créer une copie de ces cartes de transformation par défaut et modifier la carte en fonction de vos besoins. Pour plus d'informations, consultez Cartes de transformation .

Onglet Transformation



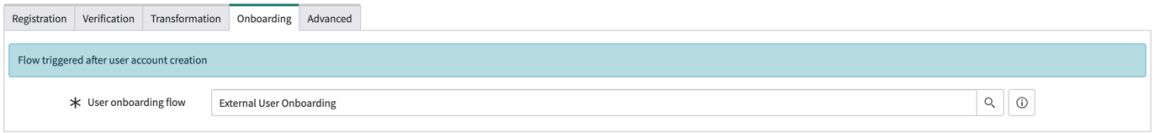
7. Configurez l'onglet **Intégration** pour déclencher des flux secondaires pour les utilisateurs activés lors de l'intégration.
   Le flux secondaire **d'intégration de l'utilisateur externe** par défaut envoie un e-mail à l'utilisateur contenant un lien pour réinitialiser son mot de passe. Vous pouvez créer une copie du flux secondaire par défaut et le modifier en fonction de vos besoins.

Remarque :
Lorsque le flux secondaire **Intégration d'un utilisateur externe** se déclenche, il envoie un e-mail à l'utilisateur contenant un lien pour réinitialiser le mot de passe.

Traduction automatique

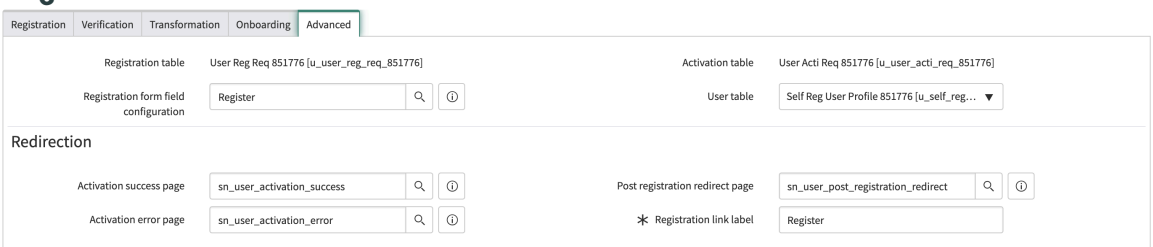
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Intégration



8. **Facultatif :** Configurez l'onglet **Avancé** pour mapper les tables d'utilisateurs et les pages de redirection du formulaire d'inscription.

Onglet Avancé



Onglet Avancé

Champ	Description
Table d'inscription	Nom de la table où les informations du formulaire d'inscription sont enregistrées.
Configuration du champ du formulaire d'inscription	Enregistrement associé au formulaire d'inscription dans le Créateur d'enregistrement.
Table d'activation	Étiquette et nom de la table utilisée pour l'activation de l'utilisateur. La table d'activation contient les enregistrements des utilisateurs qui ont effectué la vérification.
Table des utilisateurs	Étiquette et nom de la table du profil d'utilisateur.
Page de réussite d'activation	Page vers laquelle un utilisateur est redirigé après la réussite de l'activation.
Page d'erreur d'activation	Page vers laquelle un utilisateur est redirigé en cas d'échec de l'activation.
Page de redirection post-inscription	Page vers laquelle l'utilisateur est redirigé après l'inscription.
Étiquette de lien d'inscription	Nom du bouton utilisé pour l'inscription à partir du portail de services. La valeur par défaut est Register.

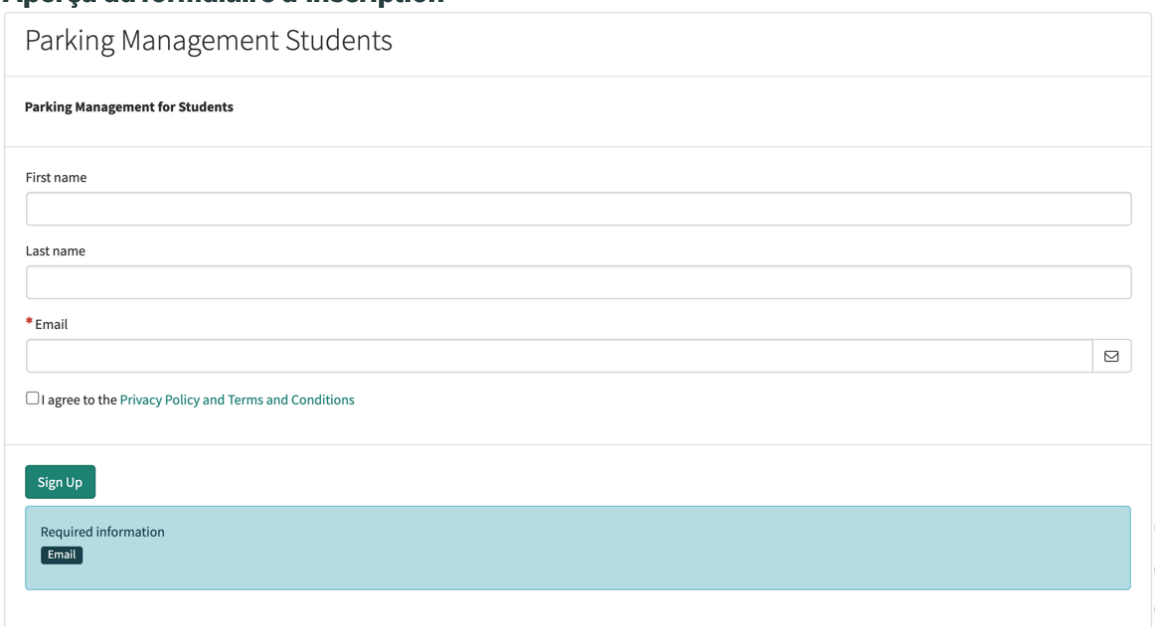
Lorsque vous apportez des modifications ou après avoir effectué toutes les modifications apportées à la configuration de l'inscription de l'utilisateur, vous pouvez utiliser le bouton

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du formulaire d'inscription pour prévisualiser les modifications apportées au formulaire d'inscription.

Aperçu du formulaire d'inscription



Configurer pour l'auto-inscription Google reCAPTCHA de l'utilisateur externe

Pour utiliser le Google reCAPTCHA service, vous devez demander une paire de clés API auprès des Google propriétés système associées, puis configurer les propriétés système connexes.

Avant de commencer

- Demander une paire de clés API (une clé de site et une clé secrète) à partir d'un Googlehttps://www.google.com/recaptcha .
- Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.
2. Recherchez les propriétés suivantes et définissez les valeurs :

Propriété	Valeur
glide.user.registration.google.recaptcha.secret	Le secret autorise la communication entre l'application et le serveur reCAPTCHA. Type : password2
glide.user.registration.google.recaptcha.site_key	Clé de site utilisée pour appeler le service reCAPTCHA sur votre page d'inscription. Type : chaîne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Valeur
glide.user.registration.captcha.widget	La Sys_ID du widget captcha. Type : chaîne

Champs de formulaire d'inscription par défaut

Vous pouvez utiliser les champs de formulaire d'inscription par défaut ou créer des champs de formulaire d'inscription personnalisés.

Champs du formulaire d'inscription

Les champs de formulaire suivants sont ajoutés par défaut au formulaire d'inscription.

Étiquette de champ	Type
Tél. professionnel	Texte sur ligne unique
Ville	Texte sur ligne unique
Pays	Zone de sélection
État d'EDU Utilisé pour différencier le personnel, les étudiants et les visiteurs. **Remarque :** Ce champ est utile lorsque le formulaire d'inscription est destiné à un établissement d'enseignement.	Zone de sélection
E-mail	E-mail
Prénom	Texte sur ligne unique
Sexe	Texte sur ligne unique
Téléphone personnel	Texte sur ligne unique
Langue	Zone de sélection
Nom de famille	Texte sur ligne unique
Deuxième prénom	Texte sur ligne unique
Tél. mobile	Texte sur ligne unique
Nom	Texte sur ligne unique
Préfixe Titre de l'utilisateur. Par exemple, M. , Dr. , et ainsi de suite.	Zone de sélection
État/Province	Texte sur ligne unique
Rue	Texte sur ligne unique large
Titre : fonction	Zone de sélection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de champ	Type
Code postal	Texte sur ligne unique

Remarque :
Vous ne pouvez pas supprimer les champs de formulaire d'inscription par défaut.

Ajouter un champ de formulaire d'inscription personnalisé

Vous pouvez ajouter des champs personnalisés dans le formulaire d'inscription automatique de l'utilisateur.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Enregistrement utilisateur externe automatique** > **Configurations de l'inscription de l'utilisateur**.
2. Ouvrez l'enregistrement pour la configuration d'inscription de l'utilisateur requise.
3. Accédez à la fin de la section Champs du formulaire d'inscription et cliquez sur **Insérer une nouvelle ligne...**.
4. Entrez le nom du champ sous la colonne **Étiquette** et cliquez sur coche.
   Une nouvelle ligne est ajoutée avec les valeurs par défaut. Vous pouvez configurer le champ de formulaire d'inscription personnalisé en fonction de vos besoins.

Colonnes du champ de formulaire d'inscription

Colonne	Description
Étiquette	Nom du champ qui apparaît sur le formulaire d'inscription.
Type	Type de l'élément d'interface utilisateur. Les types pris en charge sont les suivants : ○ Texte sur ligne unique ○ E-mail ○ Date ○ Date/Heure ○ Oui/Non ○ Texte sur ligne unique large ○ Choix multiple ○ Zone de sélection
Afficher dans le formulaire d'inscription	Option permettant d'afficher le champ dans le formulaire d'inscription.
Ordre	Séquence dans laquelle les champs de formulaire apparaissent sur le formulaire d'inscription. Le champ présentant la valeur d'ordre la plus basse apparaît en premier et le champ présentant la valeur d'ordre la plus élevée apparaît en dernier. La valeur par défaut est 10 000.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
Obligatoire	Option pour rendre un champ obligatoire sur le formulaire d'inscription.
Champ de validation uniquement	Option permettant d'utiliser un champ uniquement à des fins de validation. Par exemple, le code d'inscription. Lorsque la valeur est définie sur vrai, ce champ n'est pas enregistré dans la table utilisateur (sys_user).

5. Enregistrez ou mettez à jour les changements.

Activer l'auto-inscription de l'utilisateur externe pour Portail de services

Autorisez les utilisateurs externes à s'inscrire à une application ServiceNow via Portail de services.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Portail de services** > **Portails**.
2. Ouvrez un enregistrement de portail.
3. Renseignez le champ de **configuration de l'inscription de l'utilisateur externe** sur le formulaire.

   Sélectionnez une configuration d'inscription de l'utilisateur.
4. Cliquez sur **Mettre à jour**.

Résultats

Le widget de connexion inclut un lien vers le formulaire d'inscription que vous avez configuré précédemment.

Vérifier les demandes d'auto-inscription de l'utilisateur

Une fois qu'un utilisateur s'est inscrit à partir de , Portail de services un enregistrement utilisateur est ajouté au module Demandes d'inscription. Vous pouvez afficher la liste des utilisateurs enregistrés qui se sont enregistrés avec succès dans le Portail de services .

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Enregistrement utilisateur externe automatique** > **Demandes d'enregistrements**.
   La liste des enregistrements d'utilisateurs s'affiche.
2. (Facultatif) Affichezles enregistrements individuels des utilisateurs et modifiez-les en fonction de vos besoins. Par exemple, vous pouvez changer l'état d'un formulaire d'enregistrement utilisateur **En attente** en **Traité**.

Authentification basée sur un jeton (connexions de l'utilisateur)

Améliorez le mécanisme de sécurité permettant aux utilisateurs d'accéder à un réseau à l'aide de l'authentification basée sur les jetons.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification temporelle limitée



L’authentification basée sur un jeton est un protocole qui permet aux utilisateurs de vérifier leur identité et de recevoir en retour un jeton d’accès unique.

Il permet d’améliorer le mécanisme de sécurité permettant aux utilisateurs d’accéder à un réseau.

Utiliser l’authentification par jeton Digest



L’authentification par jeton Digest transmet les informations d’identification de l’utilisateur et un jeton Digest dans un en-tête HTTP non chiffré.

Authentification temporelle limitée

Prenez en charge l’authentification limitée dans le temps pour votre ServiceNow instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’authentification limitée en temps.

Activer



Découvrez comment activer l’authentification limitée dans le temps.

Didacticiel : Authentification limitée dans le temps



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renseignez-vous sur les propriétés de l'accès Zero Trust.

Explorer Authentification temporelle limitée

Prenez en charge l'authentification limitée dans le temps pour votre ServiceNow instance.

Remarque :
L'authentification temporelle limitée est très spécifique à l'instanceServiceNow, les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Les administrateurs peuvent configurer l'authentification basée sur lien sur l'instance ServiceNow . Le lien configuré peut être partagé avec l'utilisateur par e-mail ou SMS et l'utilisateur peut utiliser ces liens pour se connecter à l'instance.

La connexion à l'instance avec ce schéma d'authentification est contrôlée via les politiques d'authentification adaptative configurées sur l'instance ServiceNow .

L'authentification basée sur le temps vous permet d'effectuer les actions suivantes :

- L'administrateur peut configurer l'authentification basée sur un lien pour l'utiliser dans un délai d'expiration.
- L'équipe d'application peut extraire la valeur de circonstance à utiliser avec le lien pour l'élément de configuration spécifique à l'aide de l'API scriptable exposée. La génération de liens sera prise en charge par l'équipe d'application.
- L'équipe d'application peut générer le lien et l'envoyer à l'utilisateur via un canal existant.
- L'utilisateur disposant du lien peut se connecter à l'instance une seule fois et dans le délai d'expiration spécifié dans le cadre de la configuration.
- Les administrateurs peuvent configurer les rôles avec peu de privilèges pour le schéma d'authentification.
- Les administrateurs peuvent appliquer la MFA pour le schéma d'authentification comme deuxième facteur d'authentification avec le lien TLA.

Activer l'authentification temporelle limitée

L'authentification limitée en temps s'active via le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs.

Avant de commencer
Rôle requis : admin

Remarque :
L'authentification temporelle limitée est très spécifique à l'instanceServiceNow, les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Time Limited Authentication (`com.snc.authenticate.time_limited_authentication`) à l'aide des critères de filtre et de la barre de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Authentification temporelle limitée par SMS : Twilio didacticiel

Configurez une authentification limitée dans le temps avec des facteurs MFA tels que SMS à l'aide de Twilio.

Avant de commencer
Rôle requis : admin

Modules d'extension requis :

- `com.snc.authenticate.time_limited_authentication` (authentification limitée dans le temps)
- `com.snc.authentication.sms_mfa` (authentification multifacteur avec SMS)

Remarque :
L'authentification limitée dans le temps (TLA) est très spécifique à l'instanceServiceNow, les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Les instructions du didacticiel fournies permettent à l'administrateur de fournir une connexion basée sur un lien avec SMS comme deuxième facteur (MFA) pour les utilisateurs ayant un rôle spécifique.

Une fois la configuration réussie, le système génère un lien, puis le partage avec l'utilisateur via un canal de notification (e-mail/SMS). En cliquant sur le lien, l'utilisateur est invité à spécifier le facteur d'e-mail ou de SMS envoyé à l'OTP en fonction du rôle d'utilisateur (configuration).

Remarque :

- TLA doit toujours être suivi de MFA et MFA doit être activé par l'administrateur à l'aide de l'authentification adaptative pour la connexion TLA. Pour en savoir plus sur la configuration de la MFA avec l'authentification adaptative, reportez-vous à la section Contexte d'authentification multifacteur.
- Le TLA doit être utilisé pour les utilisateurs qui ont des privilèges limités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Création d’une Twilio configuration.
   a. Créez un Twilio compte de test. Pour plus d'informations, consultez Twilio .
   b. Accédez à la **Tous** > **Notification** > **Administration** > **Configuration Twilio Direct**.
   c. Fournissez le **SID de compte** et le **jeton d’authentification** (créé à partir de Twilio) et sauvegardez l’enregistrement.

> **Remarque :**
> Vous pouvez créer votre propre configuration de fournisseur et l’utiliser pour TLA. Dans cet exemple, il s’agit Twilio de . Pour en savoir plus sur la création d’une configuration de fournisseur MFA, reportez-vous à la section Configurer le fournisseur MFA.

2. Configuration et activation de l’enregistrement d’authentification limitée dans le temps (TLA).
   a. Accédez à la **Tous** > **Enregistrements de configuration de l’authentification temporelle limitée** et cliquez sur **Nouveau**.
   b. Renseignez les champs du formulaire.

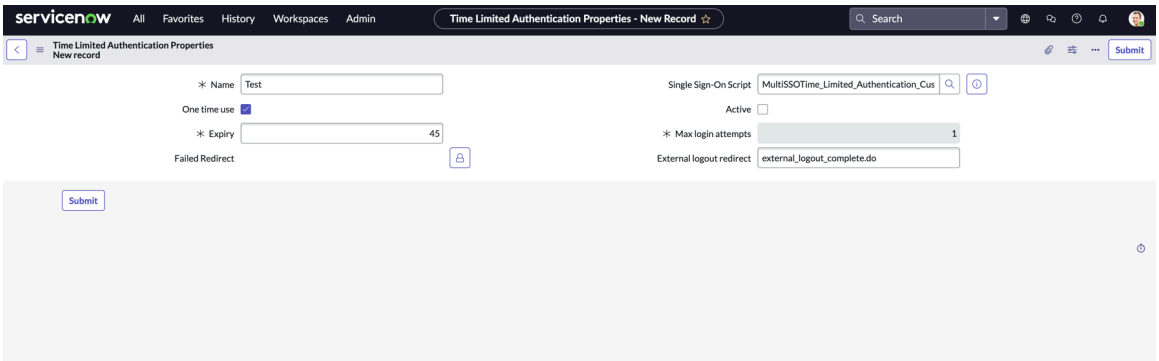
Propriétés d'authentification temporelle limitée

Champ	Description
Nom	Nom de l'enregistrement.
Utilisation ponctuelle	Activez pour utiliser le lien TLA une fois.
Expiration	Spécifiez les secondes d’expiration du lien. La valeur par défaut est de 45 minutes.
Échec de la redirection	Entrez l’URL pour rediriger des utilisateurs après un échec d’authentification.
Script d'authentification unique	Détails du script SSO que vous souhaitez utiliser.
Actif	Option permettant d’activer la configuration.
Nombre maximal de tentatives de connexion	Spécifiez le nombre de tentatives autorisées avec le lien TLA généré pour la connexion. Décochez la case **Utilisation unique** pour fournir le nombre maximal de tentatives.
Redirection de déconnexion externe	Saisissez l’URL pour rediriger les utilisateurs après la déconnexion.

   c. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Administration** > **Propriétés** et activez la propriété **Authentification unique (SSO) de plusieurs fournisseurs** et **Enregistrer**.

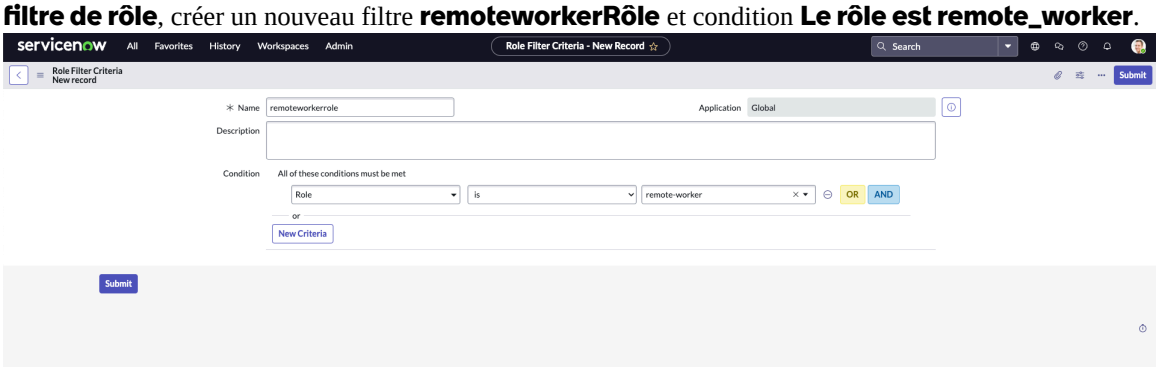
3. Autoriser TLA uniquement pour un profil d'utilisateur spécifique à l'aide de la politique de contexte de post-authentification.

a. Accédez à **Rôles** et créez un rôle. Par exemple : remote_worker.

b. Créez un utilisateur avec un ID e-mail et un numéro de téléphone portable valides. Pour savoir comment créer un utilisateur, consultez Créer un utilisateur .

c. Affectez le rôle à l'utilisateur. Pour savoir comment affecter le rôle à l'utilisateur, consultez Affecter un rôle à un utilisateur .

d. Pour créer un critère de filtre de rôle, accédez à **Tous** > **Authentification Adaptative** > **Critère de filtre de rôle**, créer un nouveau filtre **remoteworkerRôle** et condition **Le rôle est remote_worker**.

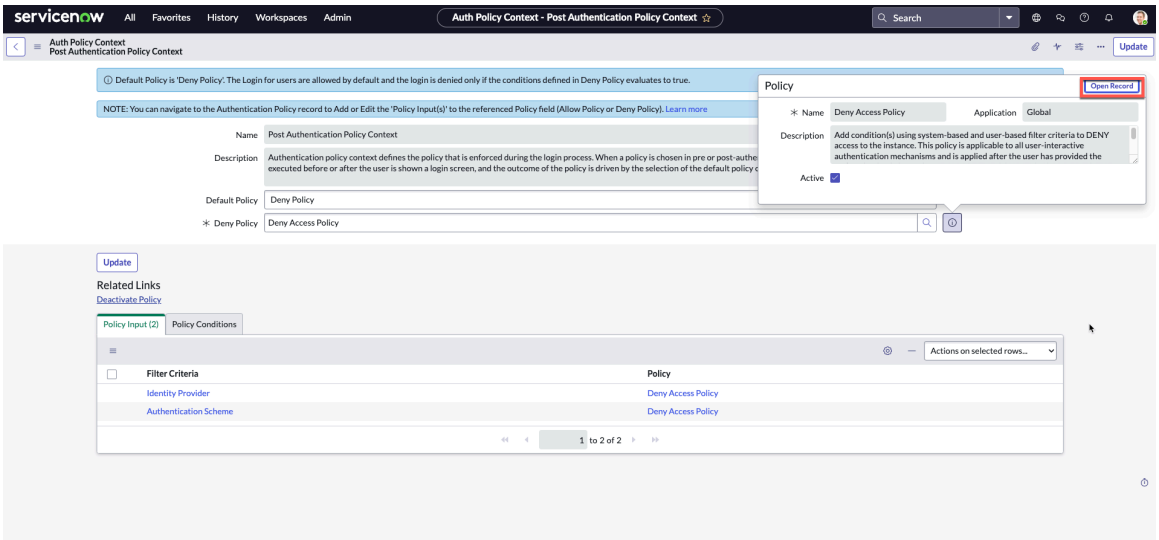


e. Pour ajouter une condition de politique basée sur le contexte de politique de refus basée sur les critères d'IdP et de filtre de rôle, accédez à **Tous** > **Authentification Adaptative** > **Contexte de post-authentification**.

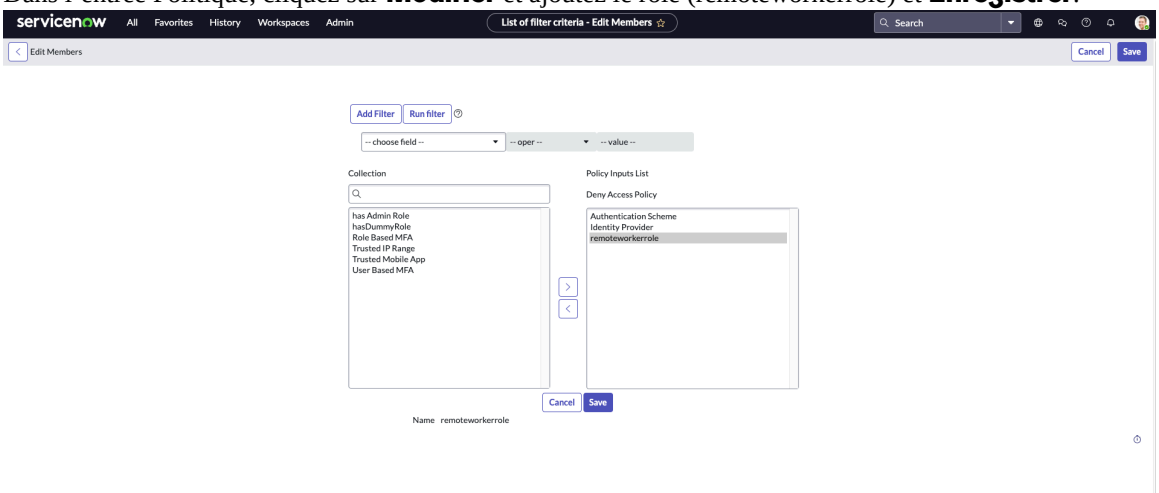
f. Cliquez sur l'icône **d'informations et ouvrez l'enregistrement**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



g. Dans l'entrée Politique, cliquez sur **Modifier** et ajoutez le rôle (remoteworkerrole) et **Enregistrer**.



h. Dans la condition de politique, ajoutez la condition pour l'entrée de politique et **soumettez** l'enregistrement.

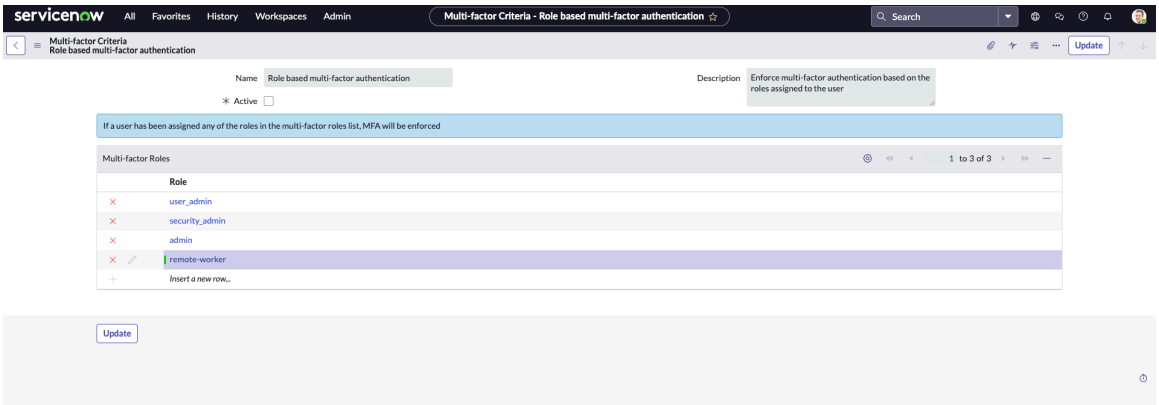
4. Configuration de la politique d'authentification renforcée : contexte MFA.

a. Accédez à la **Tous** > **Critère multifacteur**.

b. Sélectionnez **l'authentification multifacteur basée sur les rôles** et ajoutez le rôle dans la section Rôles multifacteur et **Mettre à jour**. Dans cet exemple : **remote_worker**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

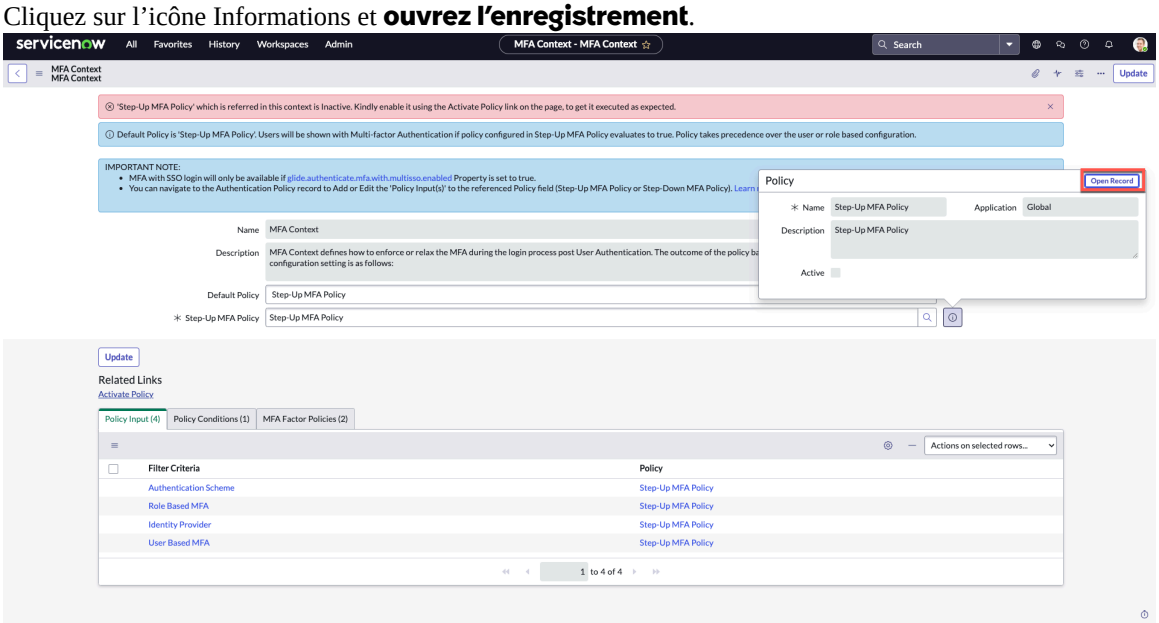


c. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte MFA**.

d. Assurez-vous de ce qui suit :

- Le champ Politique par défaut est **Politique MFA ascendante**
- La politique MFA ascendante est **une politique MFA ascendante**

e. Cliquez sur l'icône Informations et **ouvrez l'enregistrement**.



f. Dans le formulaire Politique MFA ascendante, dans Entrées de politique, cliquez sur **Modifier**.

g. Ajouter **l'authentification multifacteur basée sur les rôles** à la liste et **enregistrer**. Dans cet exemple, **rôle remoteworker.**

h. Dans la condition de politique, cliquez sur **Appliquer la MFA si les paramètres MFA basés sur le rôle ou basés sur l'utilisateur sont vrais**.

i. Sur la page Appliquer la MFA si les paramètres MFA basés sur les rôles ou basés sur l'utilisateur sont vrais, assurez-vous que **MFA basé sur les rôles** est **vrai**.

5. Application de la MFA pour utiliser SMS comme politique de facteur MFA.

Traduction automatique

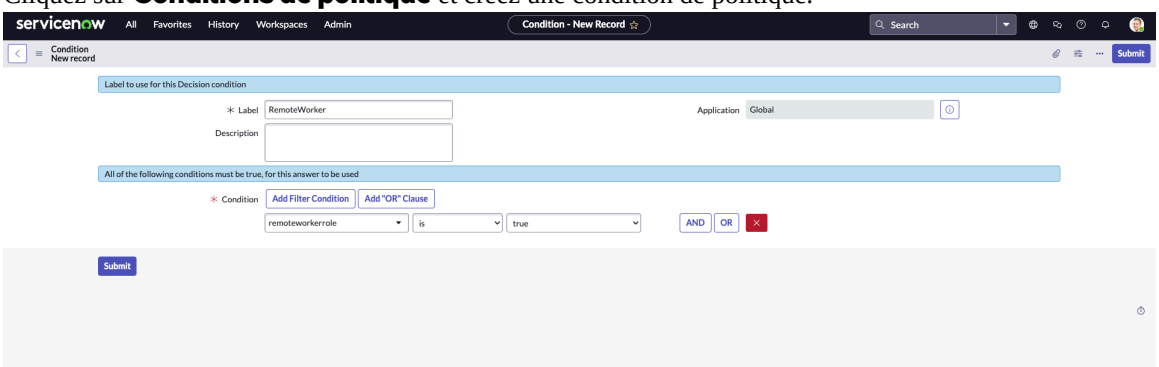
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte MFA**.

b. Sur la page Contexte MFA, cliquez sur **Politiques de facteur MFA** , puis sur politique **Afficher le mot de passe OTP SMS comme politique de facteur MFA**.

c. Cliquez sur **Modifier** et ajoutez le **rôle remoteworker** dans les **entrées de politique**.

d. Cliquez sur **Conditions de politique** et créez une condition de politique.



e. Cliquez sur **Envoyer**.

Le lien TLA généré et partagé avec les utilisateurs affectés au **rôle remoteworkerrole** sera promu pour utiliser le code SMS comme deuxième facteur pour se connecter à l'instance.

6. Activation des autres propriétés requises.

a. Accédez à la **Tous** > **Authentification multifacteur** > **Propriétés**.

b. Cochez les cases suivantes.

- **Activer l'authentification multifacteur**
- **Activer l'authentification multifacteur avec SSO**

c. Enregistrez l'enregistrement.

d. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.

e. Cochez la case **Activer la politique d'authentification** .

f. Enregistrez l'enregistrement.

7. Génération d'un lien TLA – Exemple.

a. Accédez à la **Tous** > **Définition du système** > **Scripts – Contexte**.

b. Utilisez l'API suivante en fournissant un sysid et un ID de configuration de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

var tla=new global. TimeLimitedAuthentication() ; gs.info(tla.generateNonce(« user_sysid », « config1_sys_id »,"IAR2 »)) ;

Remarque :
La source (IAR2) n'est pas un paramètre obligatoire.

c. Le paramètre de requête est renvoyé comme indiqué :
nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d344351110f8779b5

d. Créez une URL au format ci-dessous :
https://<instance-url> /login_with_sso.do ?uri=<encoded url>&
nonce=2oIlQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf03710200044e0bfc8

8. Cliquez sur l'URL, l'écran MFA suivant s'affiche pour la connexion.

Authentification par jeton Digest

L'authentification par jeton Digest transmet les informations d'identification de l'utilisateur et un jeton Digest dans un en-tête HTTP non chiffré.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l'authentification par jeton Digest.

Configurer



Découvrez comment configurer l'authentification par jeton Digest.

Explorer l'authentification par jeton Digest

L'instance lit la valeur de l'en-tête HTTP et compare sa valeur de hachage calculée du jeton de synthèse. Si la valeur de hachage calculée correspond à la valeur du jeton de synthèse, l'instance recherche une valeur correspondante dans la table Utilisateur. S'il existe une valeur correspondante dans la table Utilisateur, l'instance considère que l'utilisateur est pré-authentifié et le connecte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'authentification par jeton Digest est plus sécurisée que les simples en-têtes HTTP non chiffrés, car toute modification accidentelle ou intentionnelle de l'en-tête HTTP non chiffré produit une valeur de hachage différente. Si la valeur de hachage ne correspond pas, l'instance refuse à l'utilisateur l'accès à l'instance demandée. Cela empêche les utilisateurs de tenter de se connecter avec les informations d'identification d'un autre utilisateur.

Pour en savoir plus sur l'expiration du lien de synthèse, consultez cet article de la base de connaissances .

Remarque :
Utilisez l'authentification temporelle limitée (TLA) pour configurer des liens d'expiration basés sur le temps. Pour en savoir plus, reportez-vous à la section Authentification temporelle limitée.

Exigences d'intégration

Une intégration d'authentification par jeton Digest nécessite :

- Un serveur Web
- SiteMinder ou une autre application d'authentification unique pour pré-authentifier l'utilisateur sur le réseau local
- Page Web ou portail qui transmet les informations d'identification de l'utilisateur à l'instance cible dans l'un de ces formats
  - En-têtes HTTP
  - Paramètre d'URL
  - Cookie
- Page Web ou portail qui crée et transmet un jeton de synthèse à l'instance cible à l'aide de l'une de ces techniques de codage
  - SHA1
  - MD5
  - SHA 256 (recommandé)

Configurer les propriétés de synthèse pour l'authentification unique (SSO) de plusieurs fournisseurs

Après avoir activé un script d'installation de synthèse, configurez les propriétés de l'authentification unique (SSO) de plusieurs fournisseurs.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Si vous n'utilisez pas l'authentification unique de plusieurs fournisseurs, configurez les propriétés d'authentification unique standard.

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Remplissez les champs du formulaire Propriétés de synthèse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Nom	Entrez le nom du jeton de synthèse.
Utilisateur	Saisissez le champ sys_user qui contient les données correspondantes pour l'en-tête entrant.
Nom d'en-tête HTTP Digest	Entrez l'en-tête HTTP que vous avez généré. Par exemple, DE_USER.
Nom d'en-tête HTTP	Entrez l'en-tête HTTP que vous avez généré pour votre jeton de synthèse créé. Par exemple, SM_USER.
Phrase de sécurité secrète	Entrez la clé secrète à utiliser pour le codage des clés de synthèse. Par exemple, 32 caractères ou plus.
Échec du champ de redirection de l'authentification unique	Entrez l'URL pour rediriger des utilisateurs après un échec d'authentification.
Redirection de déconnexion externe	Saisissez l'URL pour rediriger les utilisateurs après une déconnexion.
Script d'authentification unique	Sélectionnez **MultiSSO_DigestedToken**.
Type de client	Choisissez le type de client, en fonction du type de votre client. Options :**Iframe incorporé**. **Remarque :** Si le champ Type de client est requis pour votre configuration, vous pouvez modifier le formulaire et ajouter le champ. Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

3. Cliquez sur **Mettre à jour**.
4. Définissez votre jeton digéré par défaut sur vrai.
   Lorsque vous définissez la valeur par défaut sur vrai, cela remplace l'enregistrement de jeton de synthèse par défaut du système associé à SSO. Une fois que le premier enregistrement IdP lié à l'authentification unique de plusieurs fournisseurs est activé, seuls les enregistrements associés à l'authentification unique de plusieurs fournisseurs sont utilisés.

   Les enregistrements de jeton de synthèse qui existent dans la table des propriétés de synthèse peuvent être appelés individuellement en ajoutant le Sys_ID de l'IdP. Par exemple, un enregistrement de jeton de synthèse dans l'URL d'authentification suivante : https://<instance_name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id_of_Digest_token_record>&SM_USER=<user_name>&DE_USER=<digested_token>

Exemple d'implémentations de jeton de synthèse

Voici plusieurs exemples de création d'un jeton de synthèse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'implémentations de l'authentification Digest

Synthèse générée avec	Valeur de la clé secrète	Méthode de hachage	Exemple
Java	32 caractères et plus	SHA256	Exemple d'algorithme Java Digest pour le chiffrement
C	Valeur du paramètre sharedKey	Valeur du paramètre strEncryptionMethod (SHA256 ou MD5)	Exemple C

Exemple d'algorithme de synthèse Java pour le chiffrement

Cet algorithme Java illustre la création d'un jeton de synthèse à partir d'un en-tête HTTP.

Cet exemple suppose :

- Le serveur Web prend en charge Java
- La méthode de calcul du hachage est SHA1
- La valeur de clé secrète est abc123
- Le nom de l'en-tête HTTP non chiffré est user_name

Modifiez le code Java pour utiliser un autre mécanisme de calcul de hachage (tel que MD5), modifiez la valeur de la clé secrète ou le nom de l'en-tête HTTP.

```
public class DigestTest
{
   private static final String MAC_ALG = "HmacSHA256";
     fKey  = {32 or more characters};
   public byte[] getDigest(String acct) {
      try {
         byte[] bkey = fKey.getBytes();
         byte[] data = acct.getBytes();
         Mac mac = null;
         try {
            mac = Mac.getInstance(MAC_ALG);
            mac.init(new SecretKeySpec(bkey, MAC_ALG));
         } catch (Exception e) {
            e.printStackTrace();
         }
         byte[] sig = mac.doFinal(data);
         String signature = new String(sig);
         System.out.println("value:" + acct);
         System.out.println("digested value:  " + signature);
         return sig;
      } catch (IllegalStateException e) {
         e.printStackTrace();
      }
      return null;
   }
   public static void main(String[] args) {
      BASE64Encoder encoder = new BASE64Encoder();
      DigestTest test = new DigestTest();
      String userName = "user_name";
      System.out.println("base 64 digest username: " +
encoder.encode(test.getDigest(userName)));
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    }
}
```

Exemple C

Cette classe C illustre la création d'un jeton de synthèse à partir de trois paramètres d'entrée.

- strEncryptionMethod : répertorie la méthode de calcul de hachage (SHA1, SHA256 ou MD5)
- Message : répertorie la valeur à convertir en jeton de synthèse
- sharedKey : répertorie la clé secrète

Remarque :
Utilisez un algorithme de hachage sécurisé plus fort comme SHA256 pour la génération de jetons de synthèse.

Cet exemple suppose :

- Le serveur Web prend en charge C
- D'autres codes appellent cette classe et transmettent les paramètres attendus

Exemple de code

```
private stringdigestData(string strEncryptionMethod , string message , string sharedKey ) {
        UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding ( ) ;

        byte [ ] messageBytes  = System. Text. Encoding. ASCII. GetBytes (message ) ;
        byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII. GetBytes (sharedKey ) ;
        byte [ ] hashedMessage ;

        string b64SHA1Message ;

         if (this. DEBUG ) {
           TextBoxMessage. Text = message ;
           TextBoxSecret. Text = sharedKey ; }

         switch ( (strEncryptionMethod ) )

         { case "SHA1" :

              HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
              hmacsha1. Key = sharedKeyBytes ;
              hashedMessage  = hmacsha1. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

            case "MD5" :

              HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
              hashedMessage  = hmacmd5. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

            default :
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
            b64SHA1Message  = "Unknown Encryption Method" ; break ;

        }


       TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;

    }
```

[store-future: BEGIN review]

Intégrables Web

Sécurisez la fonctionnalité d'intégrables Web pour l'authentification ServiceNow des composants Web de qui sont utilisés dans les portails tiers.

La fonctionnalité d'intégrables Web vous permet d'intégrer les ServiceNow composants Web dans des sites Web externes en dehors de ServiceNow. Vous pouvez utiliser ces composants Web pour interagir avec les API dédiées qui permettent l'échange de données en temps réel et l'utilisation ServiceNow des fonctionnalités sans que les utilisateurs aient à accéder directement à l'interface ServiceNow.

Lors de l'utilisation d'intégrables Web, il est important de s'authentifier ServiceNow aux composants Web en toute sécurité et de restreindre ou de supprimer les rôles de privilège élevé pour les utilisateurs. Pendant l'authentification, une session incorporée est établie pour afficher les informations à partir des ServiceNow composants Web.

Le point de terminaison de l'API (`/now/client/authenticate`) est utilisé pour authentifier la demande d'un tiers afin d'établir la session incorporée de ServiceNow.

Remarque :
Vous devez utiliser une URL personnalisée dédiée pour authentifier la demande d'un tiers.

Pour utiliser ce point de terminaison, vous devez envoyer un jeton JWT d'authentification au porteur valide dans l'en-tête d'autorisation dans le cadre de la demande d'authentification. Lorsqu'un jeton valide est envoyé, la session est considérée comme incorporée avec la suppression des rôles d'administrateur et d'administrateur de sécurité pour l'utilisateur.

En outre, vous pouvez effectuer une relégation de rôle pour configurer davantage les rôles qui doivent être supprimés pendant une session incorporée. Pour en savoir plus sur la configuration des rôles de session intégrés, reportez-vous à la section Configurer le rôle d'accès à la session du client.

Pour en savoir plus sur la configuration des intégrables Web, reportez-vous à la section Configure Web Embeddables .

Par défaut, la politique peut être configurée uniquement avec des critères de filtre **de session incorporés** . Vous pouvez tirer parti du plugin **Zero Trust Access (ZTA)** pour améliorer encore son utilisation avec des filtres tels que l'adresse IP, l'emplacement, le rôle, le groupe, l'identité, les attributs du fournisseur. Vous pouvez ajouter ces filtres aux politiques créées dans la table **Configuration du rôle d'accès client** . Cela permet de renforcer encore la complexité de l'accès et d'avoir une meilleure posture de sécurité lors de l'établissement d'une session intégrée. Pour plus d'informations sur ZTA, reportez-vous à la section Accès zéro confiance (ZTA).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le module d'extension Accès client intégré (com.glide.security.client_access) permet d'inclure des options telles que la relégation de rôle pour la fonctionnalité Web Intégrables. Ce module d'extension est installé automatiquement lorsque le module d'extension Web Embeddable est installé.
- Vous devez définir **la propriété glide.uxf.lib.embeddables.enabled** sur vrai pour utiliser le point de terminaison (/now/client/authenticate).

Vous pouvez également implémenter ces mesures de sécurité supplémentaires pour avoir un contrôle plus fort sur les privilèges de l'utilisateur lors de l'utilisation des composants Web :

- Configurez le type de client sur **Incorporé** pour l'enregistrement OIDC (entité OAuth) correspondant. Pour définir le type de client sur **Intégré**, vous devez installer le module d'extension **Accès zéro confiance (ZTA).**
- Utilisez **IsEmbeddedSession** comme attribut de sécurité pour les contrôles d'accès (ACL). L'attribut de sécurité **IsEmbeddedSession** est ajouté lors de l'installation du module d'extension Embedded client access (com.glide.security.client_access). Pour plus d'informations, consultez Attributs de sécurité OOB (prêts à l'emploi).

[End]
[store-future: BEGIN review]

Configurer le rôle d'accès à la session du client

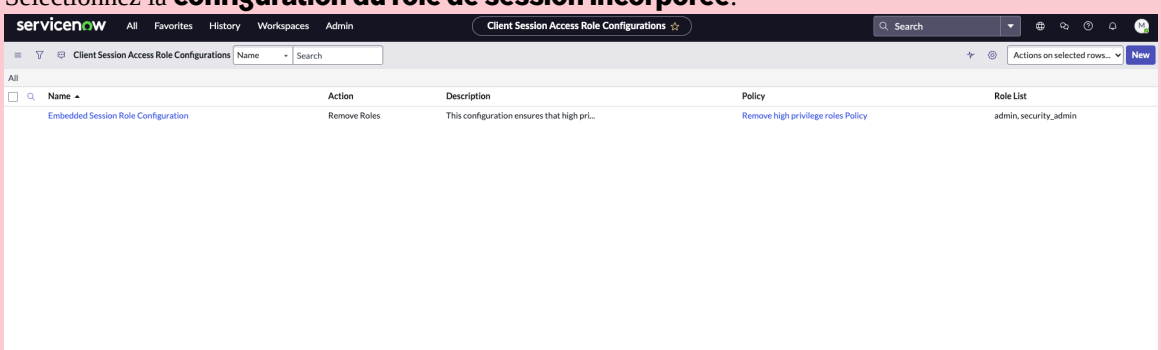
L'enregistrement **de configuration du rôle de session incorporé** (configuration du rôle d'accès client) est créé par défaut, ce qui inclut la suppression des rôles d'administrateur et d'administrateur de sécurité (rôles à privilège élevé) pour les utilisateurs utilisant les composants d'interface utilisateur sur les portails tiers.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Accès client** > **Configurations des rôles d'accès client**.
2. Sélectionnez la **configuration du rôle de session incorporée**.



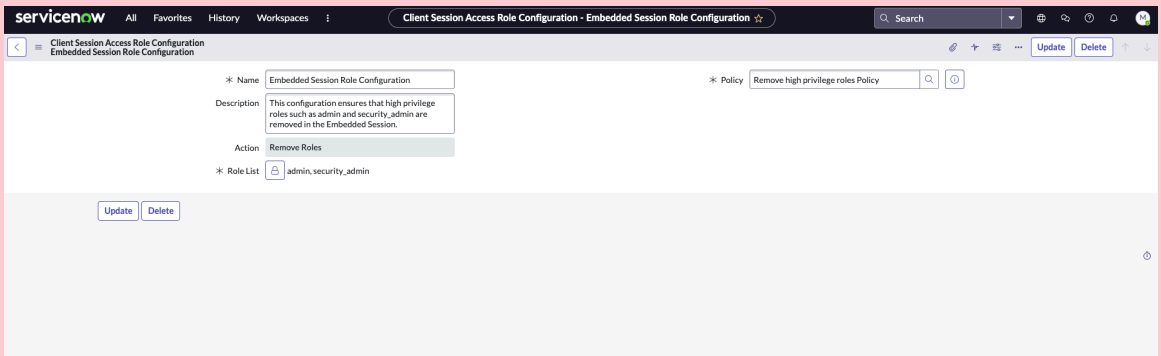
Remarque :

L'enregistrement de **configuration du rôle de session incorporé** est créé par défaut pour supprimer les rôles d'administrateur et d'administrateur de sécurité (rôles avec des privilèges élevés) des utilisateurs de la session incorporée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

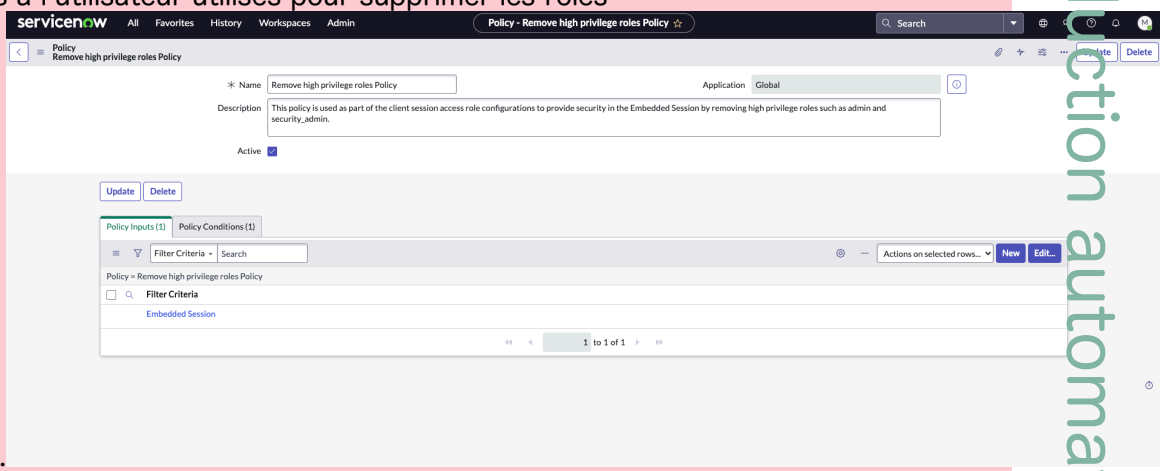
Les détails de la configuration s'affichent. Par défaut, la configuration garantit que les rôles de privilège élevé tels que **admin** et **security_admin** sont supprimés dans la session incorporée.



Vous pouvez ajouter d'autres utilisateurs à la liste en fonction de vos besoins.

3. Utilisez l'icône d'informations pour ouvrir la politique.
La politique (Politique de suppression des rôles de privilège élevé) contient les détails suivants :

   - **Entrées de politique** : Session incorporée : critères de filtre spécifiques à l'utilisateur utilisés pour supprimer les rôles configurés.



   - **Conditions de politique** : Supprimer les rôles de privilège élevé dans la session incorporée : la validation de la condition est vrai pour supprimer les rôles de privilège élevé ajoutés pour la configuration.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque l'utilisateur accède aux ServiceNow composants dans le portail tiers, en fonction des configurations ci-dessus, les rôles de privilège élevé sont supprimés pour cette session incorporée.

Vous pouvez également ajouter d'autres rôles à supprimer à cet enregistrement **de configuration de rôle de session incorporée** .

[End]

Sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de la sécurité WS.

Découvrir la sécurité Web



Découvrez les fonctionnalités et les valeurs commerciales de la sécurité des services Web.

Configurer l'authentification réciproque



Utilisez l'authentification réciproque pour établir la confiance en échangeant des certificats SSL (Secure Sockets Layer).

Traduction automatique

Découvrir la sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de la sécurité WS.

Authentification de base

Pour appliquer l'authentification de base à chaque demande de document WSDL ou de publication de messages SOAP, vous pouvez définir la propriété *`glide.basicauth.required`* sur `true`. Dans ce cas, chaque demande WSDL ou SOAP doit contenir l'en-tête « Autorisation » comme spécifié dans le protocole d'authentification de base . Étant donné que la demande n'est pas interactive, l'en-tête **Authorization** est toujours requis au cours d'une demande.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fournir des informations d'authentification de base, qu'elles soient requises ou non, présente l'avantage supplémentaire que les données créées ou mises à jour à la suite de l'invocation du service Web sont effectuées au nom de l'utilisateur fourni dans les informations d'identification d'authentification de base. Par exemple, lors de la création d'un enregistrement d'incident, les champs de journal utilisent l'ID d'utilisateur de l'utilisateur authentifié de base au lieu de l'utilisateur **invité** par défaut.

Pour que l'en-tête d'autorisation ignore les règles de capitalisation, utilisez la *`glide.security.script.include.name.case.insensitive.list`* propriété. Vous pouvez modifier cette propriété dans la table Propriétés système [sys_properties] et ajouter les includes de script nécessaires au traitement de l'authentification. Par défaut, cette propriété comporte les valeurs suivantes :

- BasicAuth
- CustomAuth

Ajoutez d'autres includes de script si nécessaire.

Pour fournir une authentification de base lors de l'utilisation de Perl et des bibliothèques SOAP ::Lite, vous pouvez implémenter la fonction suivante :

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' =>
 'password' ; }
```

- Lorsque vous utilisez C# .NET VS 2005 ou une version antérieure, vous pouvez tirer parti de l'objet Informations d'identification, par exemple :

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential ( "user_name",
 "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception ex ) { }
```

- Lorsque vous utilisez C# .NET VS 2008, vous pouvez tirer parti de l'objet ClientCredentials, par exemple :

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService . Demo_Incident .
 ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

  Ensuite, dans votre fichier app.config, recherchez ce qui suit et remplacez `Aucun` par `Basique` :

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```

- Lors de l'utilisation de VB .NET, tirer parti de l'objet Informations d'identification ressemblerait à ce qui suit :

```
Sub Main()
        Dim cred  As New System.Net.NetworkCredential( "user_name",  "password")

        Dim proxy  As New VB_Democm.incident.ServiceNow
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
      Dim getIncident  As New VB_Democm.incident. get Dim getResponse  As New
VB_Democm.incident.getResponse

      proxy.Credentials = cred

      getIncident.sys_id =  "[your sysID here]"

      getResponse = proxy. get(getIncident)

   End Sub
```

La réponse obtenue lorsque l'authentification de base est activée et qu'aucune information d'identification n'est fournie ressemble à ceci :

```
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </ title > <style > <!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
 H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}
 H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
   BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;}
 B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}    P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}   A
{color : black;}   A.name {color : black;}   HR {color : #525D76;}--> </
style > </ head > <body > <h1 >HTTP Status 401 -\ </ h1 > <HR size = "1" noshade =
"noshade" > <p >< b >type </ b > Status report </ p > <p >< b >message </ b > <u >< /
u >< / p > <p >< b >description </ b > <u >This request requires HTTP authentication ().
</ u >< / p > <HR size = "1" noshade = "noshade" > <h3 >Apache Tomcat/5.0.28 </ h3 >
</ body > </ html >
```

Configurer l'authentification réciproque

L'authentification réciproque établit la confiance en échangeant des certificats SSL (Secure Sockets Layer).

Lors de la poignée de main SSL, le serveur présente son certificat au client. Par la suite, en fonction de la configuration du serveur, il peut demander un certificat au client. Le serveur et le client exécutent des procédures de validation de certificat pour garantir l'authenticité et l'intégrité des certificats présentés.

Après une validation réussie, les accusés de réception sont échangés avant le lancement de la connexion HTTPS.

Remarque :
Pour plus d'informations sur l'utilisation d'un profil de protocole HTTPS personnalisé pour activer l'authentification réciproque, reportez-vous à la section Create a protocol profile .

Les administrateurs effectuent le travail préliminaire de configuration du magasin de clés client et de génération des certificats avant que les demandes de certification ne soient satisfaites.

Avertissement :
Cette fonctionnalité active uniquement l'authentification réciproque sur les connexions https sortantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création du magasin de clés

L'instance prend actuellement en charge le chargement d'un fichier Java Key Store, qui contient une clé privée et une paire de certificats publics, le certificat public inclut une chaîne complète, y compris le certificat racine.

Pour configurer votre magasin de clés client :

- Vous avez besoin d'un certificat signé par une autorité de certification (CA) approuvée.
- Votre fournisseur de point de terminaison d'API peut vous aider à générer le magasin de clés.

Si vous devez générer le magasin de clés, le processus implique plusieurs étapes à l'aide de commandes d'interface de ligne de commande pour générer un nouveau fichier de magasin de clés, créer une demande de signature de certificat (CSR) et importer des certificats signés. Avant d'importer le certificat principal de votre domaine, tous les certificats racines ou intermédiaires doivent d'abord être importés. Voici une instruction étape par étape :

1. Générez un magasin de clés Java et une paire de clés.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Générez une CSR pour un magasin de clés Java existant.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Envoyez la CSR à votre signataire autorisé d'autorité de certification pour signer et renvoyer les fichiers de certificat, qui comprennent les certificats intermédiaires et racines, ainsi que le certificat signé.
4. Importez un certificat d'autorité de certification (CA) racine ou intermédiaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

Remarque :
Vous pouvez regrouper tous les certificats dans un seul fichier et les importer. C'est une option préférable. Si vous procédez de cette façon, vous pouvez ignorer 5

```
keytool -import -alias mydomain -file merged.crt -keystore my.keystore
```

5. Importez un certificat primaire signé dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Configuration du magasin de clés

Maintenant que le magasin de clés a été créé, il peut être téléchargé dans la table Certificats. Sur le **Définition du système** > **Certificats** , cliquez sur **Nouveau** et définissez les champs suivants :

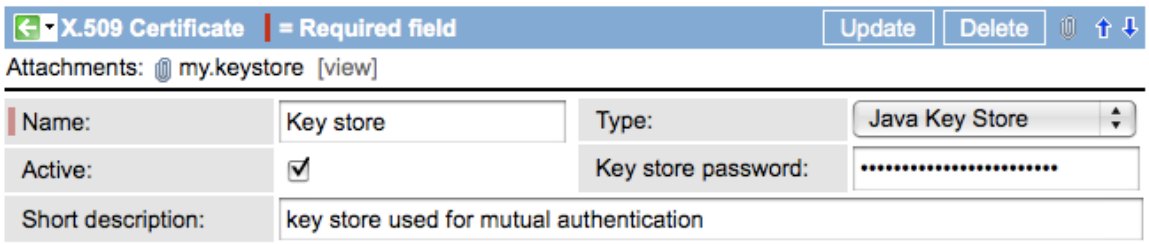
- Entrez un **nom** de certificat.
- Stockez le magasin de clés en **tant qu'actif**.
- **Définir le type = Magasin de clés Java**.
- Fournissez un **mot de passe de magasin de clés**. Il s'agit du mot de passe utilisé pour créer le magasin de clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur **Soumettre** pour créer l'entrée Java Key Store.

Magasin de clés



Spécification d'un certificat de serveur de confiance

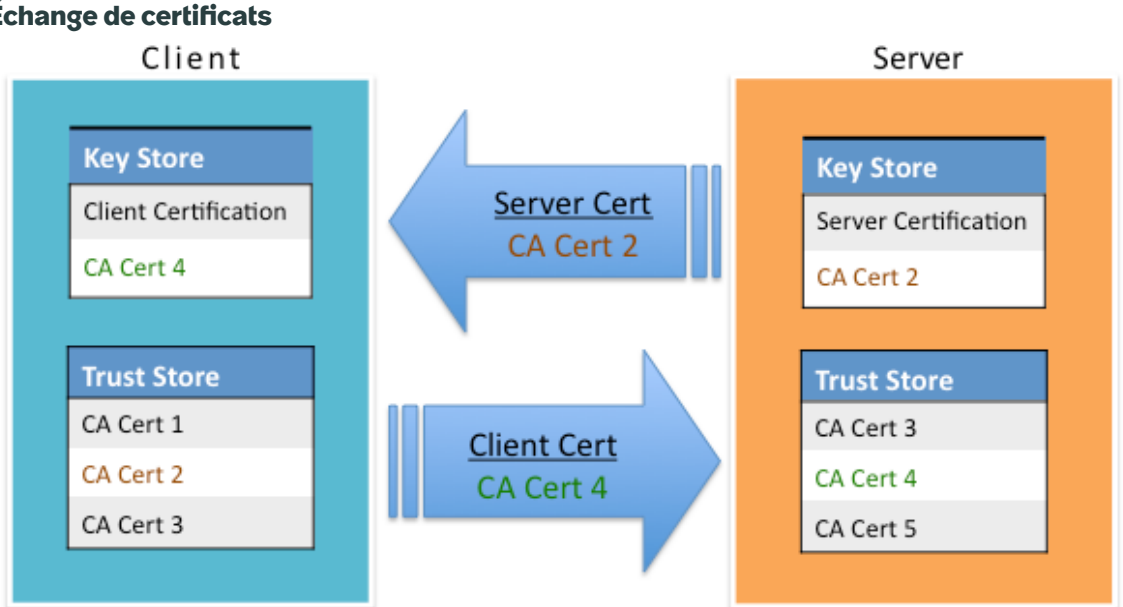
Lors d'une connexion SSL sortante, qui est un appel de service web HTTPS, il est possible de spécifier un certificat fourni par le fournisseur de service qui assure la validité du fournisseur de service pendant la connexion SSL. Par exemple, un navigateur qui tente de se connecter à un service sécurisé et qui s'identifie par un certificat.

En chargeant le certificat de serveur approuvé, ServiceNow assurez-vous que le service auquel il se connecte est valide et sécurisé.

Créez une nouvelle entrée de certificat avec le type de « Certificat de magasin de confiance » et joignez un certificat au format DER, ou copiez-collez son format PEM dans le champ **Certificat PEM** .

Profil du protocole

Échange de certificats



- Lorsqu'un client demande le certificat du serveur pour l'authentification, une demande de signature de certificat (CSR) est générée.
- Pour répondre à une CSR, le serveur génère deux clés cryptographiques uniques : une clé publique, qui est utilisée pour chiffrer les messages vers le serveur et une clé privée, qui est utilisée pour déchiffrer les messages. Les deux clés sont conservées dans le magasin de clés.
- Les clés sont utilisées pour déchiffrer les messages sécurisés du client afin qu'ils puissent être lus par le serveur. Toute connexion sortante au format HTTPS vérifie la certification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en vérifiant le magasin de clés, en offrant sa certification publique, et utilise les certificats du magasin de clés de confiance pour vérifier la confiance mutuelle.

- Pour compléter le lien sécurisé entre le client et le serveur, le serveur associe le certificat à la clé privée correspondante. Étant donné que seul le serveur a accès à la clé privée, il peut déchiffrer les données du client.

Remarque :
Pour plus d'informations sur l'utilisation d'un profil de protocole HTTPS personnalisé pour activer l'authentification réciproque, reportez-vous à la section Create a protocol profile .

Le serveur répond en envoyant un certificat. S'agit-il d'un certificat accepté par le client ? Si oui, un message d'acceptation du certificat est envoyé au serveur et un canal sécurisé est initié. Si le certificat n'est pas accepté, cela peut signifier que l'autorité racine est nécessaire pour la certification.

Règles de la liste de contrôles d'accès

Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Explorer les ACL



En savoir plus sur les listes de contrôle d'accès (ACL).

Configurer les ACL



Configurez les ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestionnaire de sécurité contextuelle



En savoir plus sur le gestionnaire de sécurité contextuelle.

Configuration avancée de l’ACL



En savoir plus sur les configurations et les outils avancés d’ACL.

Traduction automatique

Explorer les listes de contrôle d’accès

Explorer les listes de contrôle d’accès (ACL).

Toutes les règles de la liste de contrôle d’accès spécifient :

- Le *type de décision*, le *type de règle* et l’opération qui définissent l’ACL
- *Objet* en cours de sécurisation
- *Conditions requises* pour accéder à l’objet

Composants d’ACL

Le type de décision définit si les utilisateurs sont autorisés à accéder à l’objet si les conditions sont remplies ou s’ils refusent l’accès à l’objet si les conditions ne sont pas remplies.

Type de décision	Description
Refuser sauf	Restreignez l’accès à la ressource en refusant explicitement l’accès, sauf si certaines conditions sont respectées. Consultez #unique_1489_Connect_42_section_qnd_snl_zbc pour plus d'informations.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de décision	Description
Autoriser si	Autorisez l'accès à la ressource si les conditions sont vérifiées.

L'objet est la cible à laquelle l'accès doit être contrôlé. Chaque objet se compose d'un type et d'un nom qui identifient de manière unique une table, un champ ou un enregistrement particulier. Avec le champ *S'applique,* les utilisateurs disposent d'un contrôle granulaire sur les enregistrements spécifiques auxquels cette ACL s'appliquera.

Par exemple, toutes ces entrées spécifient un objet :

Type	Nom	Objet sécurisé
record	[incident]. [--Aucun--]	La table Incident.
record	[incident]. [actif]	Le champ Actif de la table Incident.
record	[incident] S'applique à : priorité = P1	Uniquement les incidents de priorité 1 dans la table des incidents.
REST_Endpoint	user_role_inheritance	Enregistrement de l'API REST user_role_inheritance scriptée.

Chaque *opération* décrit une *action* valide que le système peut entreprendre sur l'objet spécifié. Certains objets, tels que les enregistrements, prennent en charge plusieurs opérations, tandis que d'autres, tels qu'un REST_Endpoint, ne prennent en charge qu'une seule opération.

Par exemple, toutes ces entrées spécifient une opération :

Type	Nom	Opération	Opération sécurisée
record	[incident]. [-- Aucun --]	créer	Création d'enregistrements dans la table Incident.
record	[incident]. [actif]	écrire	Mise à jour du champ Actif dans la table Incident.
REST_Endpoint	user_role_inheritance	exécuter	Exécution de l'API REST user_role_inheritance scriptée.

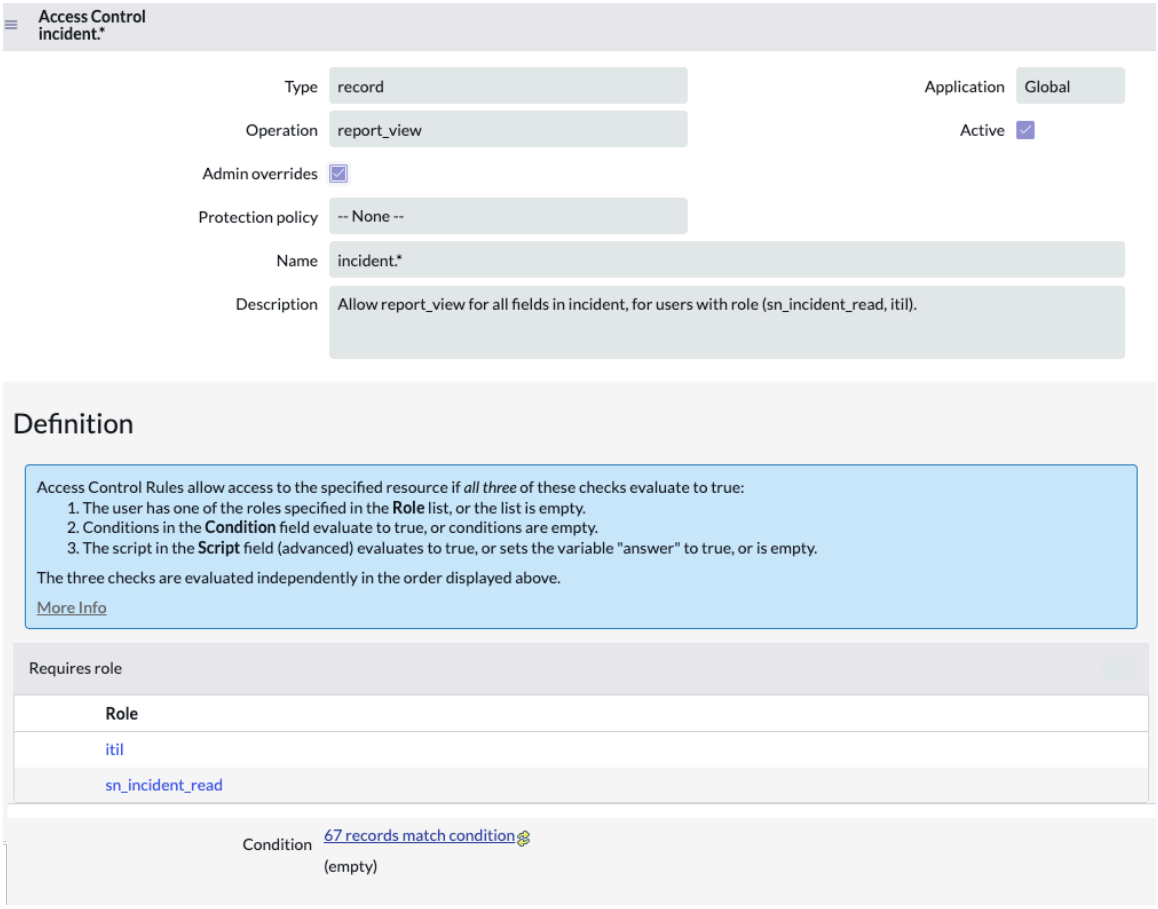
Les *conditions* spécifient quand une personne peut accéder à l'objet et à l'opération nommés. Les administrateurs de sécurité peuvent spécifier les exigences de condition en ajoutant :

- Un ou plusieurs rôles d'utilisateur dans la liste **Exige un rôle** .
- Un ou plusieurs attributs de sécurité doivent être évalués pour être vrais.
- Une ou plusieurs conditions de données.
- Script qui évalue vrai ou faux, ou qui définit la variable de `réponse` sur vrai ou faux.

Pour accéder à un objet et à une opération, un utilisateur doit satisfaire à toutes les conditions répertoriées dans un contrôle d'accès. Par exemple, ce contrôle d'accès restreint l'accès aux opérations d'affichage sur la table d'incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour mettre à jour un enregistrement dans la table d'incidents, un utilisateur doit disposer des rôles répertoriés et l'enregistrement doit remplir la condition.

Type de condition	Besoin	Description
Demande un rôle	**Nécessite un rôle** : itil	Autoriser uniquement les utilisateurs ayant le rôle itil à mettre à jour les incidents.
Attributs de sécurité	UserIsAuthenticated	Uniquement les utilisateurs authentifiés pour mettre à jour les incidents.
Condition de données	[État de l'incident] [n'est pas] [Fermé]	Autorisez uniquement les mises à jour des enregistrements d'incidents actifs.

S'applique au comportement

Le champ *S'applique à* détermine si une ACL s'applique aux enregistrements, tandis que la condition de données évalue une ACL déjà appliquée. *S'applique à* spécifie si l'ACL affecte un enregistrement spécifique ; si elle est vide, l'ACL s'applique à tous les enregistrements. *S'applique à* peut être utilisé pour l'application granulaire des ACL, tandis que « Condition de données » est un critère d'évaluation.

Remarque :
S'applique à est sensible à la casse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Refuser le comportement par défaut

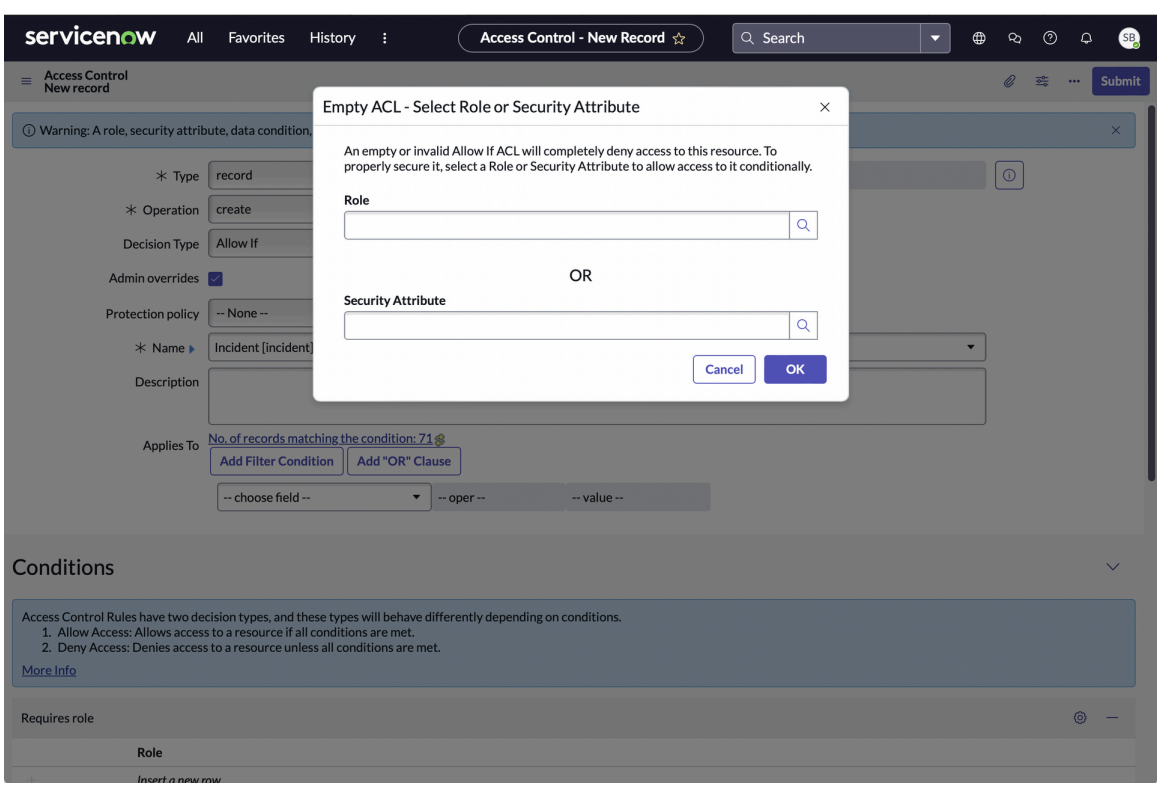
Par défaut, le moteur ACL refuse complètement l'accès si une ACL est vide ou invalide. Les ACL vides sont définies comme des ACL sans un ou plusieurs de ces composants :

- Rôle défini
- Attribut de sécurité
- Condition de données
- Script

Les ACL non valides sont définies comme :

- ACL ayant des rôles qui n'existent pas (par exemple, qui n'ont pas de ligne dans la base de données)
- ACL avec des attributs de sécurité qui n'existent pas (par exemple, qui n'ont pas de ligne dans la base de données)
- ACL avec un script qui contient « answer=true » ou « true »

Si le système détecte que l'utilisateur crée une ACL, il l'invite à sélectionner un rôle ou un attribut de sécurité existant.



Processus d'évaluation ACL

Une règle ACL n'accorde à un utilisateur l'accès à un objet que si l'utilisateur remplit toutes les conditions requises par la règle ACL correspondante.

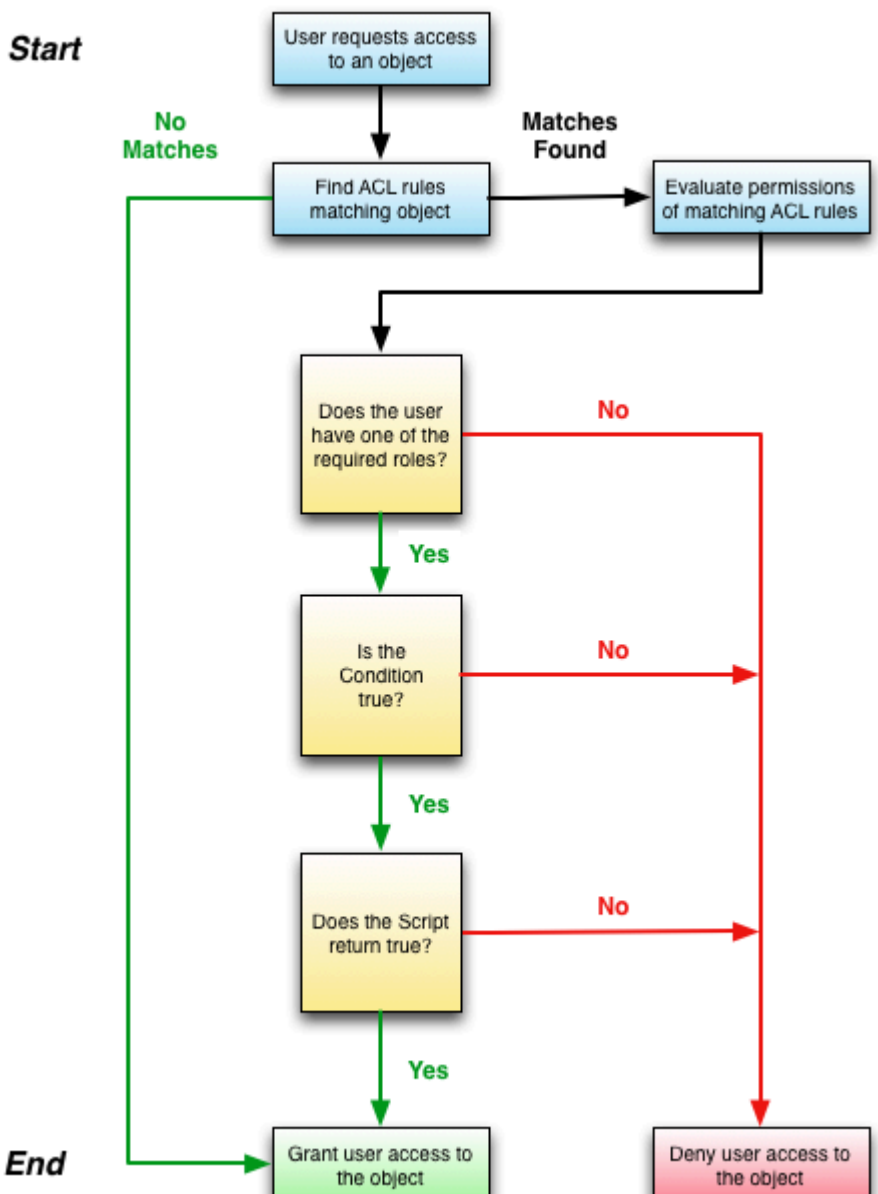
- La condition doit être évaluée *comme vraie*.
- Le script doit être *évalué comme vrai* ou renvoyer une variable de réponse avec la valeur *vrai*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'utilisateur doit disposer de l'un des rôles de la liste des rôles requis. Si la liste est vide, cette condition est évaluée *comme vraie*.
- [Règles ACL d'enregistrement uniquement] Les règles ACL au niveau de la table et au niveau du champ correspondantes doivent toutes deux être évaluées sur *vrai*.

Conditions d'évaluation ACL



Chaque fois qu'une session demande des données, le système recherche des règles de contrôle d'accès qui correspondent à l'objet et à l'opération demandés. S'il existe une règle de contrôle d'accès correspondante, le système évalue si l'utilisateur possède les conditions requises pour accéder à l'objet et à l'opération. Si une règle de contrôle d'accès spécifie plus d'une condition, l'utilisateur doit remplir toutes les conditions pour accéder à l'objet et à l'opération. L'échec d'une vérification de condition empêche l'utilisateur d'accéder à l'objet et à l'opération correspondants.

Si un utilisateur ne répond pas aux conditions de la première règle de correspondance, le système évalue les conditions de la règle de contrôle d'accès suivante spécifiée par l'ordre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de traitement du contrôle d'accès. Si l'utilisateur ne remplit pas les conditions d'une règle de contrôle d'accès correspondante, le système refuse l'accès à l'objet et à l'opération demandés.

Remarque :
S'il n'existe aucune règle de contrôle d'accès correspondante pour l'objet et l'opération demandés, le système accorde à l'utilisateur l'accès à celui-ci. En pratique, il est rare que le système ne trouve aucune règle correspondante car le système dispose d'un ensemble de règles de contrôle d'accès par défaut qui protègent toutes les opérations d'enregistrement.

Les effets du refus d'accès à un objet dépendent de la règle ACL à laquelle l'utilisateur a échoué. Par exemple, l'échec d'une règle ACL d'opération de lecture empêche l'utilisateur de voir l'objet. Selon l'objet sécurisé, la règle ACL masque un champ dans un formulaire, masque des lignes dans une liste ou empêche un utilisateur d'accéder à une page de l'interface utilisateur. La table suivante contient une liste complète des résultats d'échec d'une règle ACL pour une opération et un type d'objet donnés.

Vérifications ACL avant et après requête

Votre instance vérifie les règles ACL avant et après qu'un utilisateur a effectué une requête. Étant donné que différentes informations sont disponibles avant et après une requête, les résultats peuvent être différents.

Vérification ACL pré-requête

Avant d'exécuter une requête de base de données, votre instance vérifie les règles ACL pour chaque champ de la table interrogée afin de déterminer les champs auxquels un utilisateur peut accéder. Cette vérification ne porte que sur les rôles de l'utilisateur et vérifie si ces rôles autorisent l'accès à des champs. Étant donné que cette vérification s'exécute avant la requête, l'ACL n'a pas accès aux enregistrements de la table et ne peut donc pas prendre en compte ces données. Les scripts et les conditions qui reposent sur la connaissance du contenu d'un enregistrement ne sont pas évalués.

Si l'utilisateur ne dispose pas d'un accès en lecture à ce stade, la valeur du champ ne s'affiche pas pour l'utilisateur.

Vérification ACL post-requête

Après la requête, votre instance vérifie chaque enregistrement renvoyé par la requête. Au cours de cette vérification, il existe un contexte pour l'ACL, de sorte que les parties rôle, condition et script de l'ACL sont évaluées. Si l'utilisateur ne dispose pas d'un accès en lecture à ce stade, la valeur du champ ne s'affiche pas pour l'utilisateur. Toutefois, l'utilisateur voit l'étiquette du champ si son rôle l'autorise.

Opération	Résultats de l'échec d'une règle ACL sur l'objet
exécuter	L'utilisateur ne peut pas exécuter de scripts sur un enregistrement ou une page d'interface utilisateur.
créer	L'utilisateur ne peut pas voir l'action **Nouvelle** interface utilisateur dans les formulaires. L'utilisateur ne peut pas non plus insérer d'enregistrements dans une table à l'aide de protocoles API tels que les services Web. Une ACL **de création** avec une condition exigeant qu'un champ contienne une valeur spécifique peut être évaluée comme fausse. Les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opération	Résultats de l'échec d'une règle ACL sur l'objet
	champs des nouveaux enregistrements sont considérés comme vides jusqu'à ce que l'enregistrement soit enregistré.
Lire	L'utilisateur ne peut pas voir l'objet dans les formulaires ou les listes. L'utilisateur ne peut pas non plus récupérer les enregistrements à l'aide de protocoles API tels que les services Web.
écrire	L'utilisateur voit un champ en lecture seule dans les formulaires et les listes, et l'utilisateur ne peut pas mettre à jour les enregistrements à l'aide de protocoles API tels que les services Web.
supprimer	L'utilisateur ne peut pas voir l'action **d'interface utilisateur Supprimer** des formulaires. L'utilisateur ne peut pas non plus supprimer des enregistrements d'une table à l'aide de protocoles API tels que les services Web.
edit_task_relations	L'utilisateur ne peut pas définir de relations entre les tables de tâches.
edit_ci_relations	L'utilisateur ne peut pas définir de relations entre les tables d'éléments de configuration [cmdb_ci].
save_as_template	Utilisée pour contrôler les champs qui doivent être enregistrés lorsqu'un modèle est créé.
add_to_list	L'utilisateur ne peut pas afficher ou personnaliser des colonnes spécifiques dans les réglages de liste.
list_edit	L'utilisateur ne peut pas mettre à jour les enregistrements (lignes) d'une liste.
report_on	L'utilisateur ne peut pas créer de rapport sur la table ACL. Pour plus d'informations, consultez Restreindre la création de rapports avec une règle ACL .
report_view	L'utilisateur ne peut pas afficher le contenu d'un rapport sur la table ACL ou sur le champ ACL. Pour plus d'informations, consultez Reporting .
personalize_choices	L'utilisateur ne peut pas cliquer avec le bouton droit sur un champ de liste et sélectionner **Configurer les choix**.

Exigences de correspondance ACL pour les objets

Type d'objet	Règles ACL correspondantes requises pour accéder à l'objet	Règles ACL génériques existantes
Includes de script pouvant être appelés par le client Processeurs	Les utilisateurs doivent répondre aux conditions de deux règles ACL : 1. Toutes les règles ACL génériques pour l'objet (le cas échéant, une règle ACL existe pour l'opération). 2. Première règle ACL correspondant au nom de l'objet (s'il existe une règle ACL pour l'opération).	Par défaut, il n'existe aucune règle générique (*) pour ces types d'objets. Si vous créez une règle ACL générique pour l'un de ces objets, la règle ACL s'applique à tous les objets de ce type.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d'objet	Règles ACL correspondantes requises pour accéder à l'objet	Règles ACL génériques existantes
Pages de l'interface utilisateur Enregistrement	Les utilisateurs doivent répondre aux conditions de deux règles ACL : 1. Première règle ACL qui correspond au champ de l'enregistrement (le cas échéant, une règle ACL existe pour l'opération). 2. Première règle ACL correspondant à la table de l'enregistrement (le cas échéant, une règle ACL existe pour l'opération).	Par défaut, il existe des règles de table générique (*) pour les opérations de création, de lecture, d'écriture et de suppression et des règles de champ générique (*.*) pour les opérations de personalize_choices, de création et de save_as_template. Lorsque vous créez une table, créez des règles ACL pour la table, sauf si vous souhaitez utiliser les règles ACL génériques fournies.

Remarque :
La propriété Comportement par défaut (`glide.sm.default_mode`) du gestionnaire de sécurité détermine si les utilisateurs peuvent accéder aux objets qui ne correspondent qu'aux règles ACL de table à caractères génériques. Lorsque cette propriété est définie sur *Refuser l'accès*, seuls les administrateurs peuvent accéder aux objets qui correspondent aux règles ACL de la table à caractère générique.

Remarque :
La règle ACL du champ de caractère générique (*.*) pour l'opération de création réutilise les mêmes conditions que l'opération d'écriture. Cela signifie que les conditions de création sont les mêmes que les conditions d'écriture, sauf si vous définissez une règle ACL d'opération de création explicite.

Plusieurs règles ACL au même moment dans l'ordre de traitement

Si deux règles ou plus correspondent en même temps dans l'ordre de traitement, l'utilisateur doit satisfaire à l'une des conditions de règles ACL pour accéder à l'objet. Par exemple, si vous créez deux règles ACL de champ pour `incident.number`, l'utilisateur qui transmet une règle a accès au champ numéro, qu'il ait échoué ou non à une autre règle ACL de champ au même moment de l'ordre de traitement.

Rôle requis

Les utilisateurs administrateurs normaux peuvent afficher et déboguer les règles de contrôle d'accès. Toutefois, pour créer ou mettre à jour des règles de contrôle d'accès existantes, les administrateurs doivent élever les privilèges au rôle security_admin. Consultez les Accéder à un rôle privilégié pour obtenir les instructions.

Règles ACL dans les applications incluses dans le périmètre

Vous pouvez créer des règles ACL pour des objets dans le même champ d'application que la règle ACL. Vous pouvez également créer des règles ACL pour les tables comportant au moins un champ qui se trouve dans le même champ d'application que la règle ACL.

Pour les tables dont le champ d'application est différent de celui de l'enregistrement de règle ACL, les types de règles sont limités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous pouvez créer une règle ACL pour n'importe quelle table, page d'interface utilisateur ou tout autre objet du même champ d'application que la règle ACL.
- Vous pouvez créer une ACL pour un champ qui se trouve dans le même champ d'application que la règle ACL.
  - Si la table se trouve dans le même périmètre, vous pouvez utiliser un script pour évaluer les conditions.
  - Si la table se trouve dans un périmètre différent, vous ne pouvez pas utiliser de script pour évaluer les conditions.
- Vous ne pouvez pas créer ou modifier de règles ACL pour des objets qui se trouvent dans un périmètre différent de celui de l'application que vous avez sélectionnée dans le sélecteur d'application, y compris ajouter un rôle à une ACL dans un périmètre différent.
- Vous ne pouvez créer des règles de table générique (*) que dans le champ d'application global.
- Vous pouvez créer des règles de champs génériques (*) uniquement pour les tables du même champ d'application que la règle ACL.

Types de règles ACL

Créez des règles ACL sur différents composants du système.

Enregistrer les règles ACL

Les règles ACL d'enregistrement se composent de noms de tables et de champs.

- Le nom de la table est la table que vous souhaitez sécuriser. Si d'autres tables s'étendent à partir de cette table, la table est considérée comme une table parente. Les règles ACL pour les tables parentes s'appliquent à toute table qui étend la table parente.
- Le nom du champ est le champ que vous souhaitez sécuriser. Certains champs font partie de plusieurs tables en raison de l'extension de table. Les règles ACL pour les champs d'une table parente s'appliquent à toute table qui étend la table parente.

Les règles ACL peuvent sécuriser les opérations d'enregistrement suivantes :

Opération	Description
exécuter	Permet aux utilisateurs d'exécuter des includes de script pouvant être appelés par le client et l'exécution du point de terminaison REST.
query_match	Permet aux utilisateurs de soumettre des requêtes de correspondance (« est », « n'est pas », « est vide », etc.).
conditional_table_query_range	Permet aux utilisateurs de donner un accès partiel aux ACL en fonction des ACL en lecture. Créé pour les tables qui ont les ACL de lecture sans condition de données ni script.
query_range	Permet aux utilisateurs de soumettre des requêtes de plage (« commence par », « se termine par », « contient », etc.) et le tri est illimité.
créer	Permet aux utilisateurs d'insérer de nouveaux enregistrements (lignes) dans une table.
Lire	Permet aux utilisateurs d'afficher les enregistrements d'une table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opération	Description
écrire	Permet aux utilisateurs de mettre à jour les enregistrements d'une table.
supprimer	Permet aux utilisateurs de supprimer des enregistrements d'une table ou d'abandonner une table.
edit_task_relations	Permet aux utilisateurs d'étendre la table Tâche [task].
edit_ci_relations	Permet aux utilisateurs d'étendre la table d'éléments de configuration [cmdb_ci].
save_as_template	Permet aux utilisateurs d'enregistrer un enregistrement en tant que modèle.
add_to_list	Empêche les utilisateurs d'afficher ou de personnaliser des colonnes spécifiques dans la mécanique de liste. **Remarque :** Les conditions et les scripts ne sont pas pris en charge.
list_edit	Permet aux utilisateurs de mettre à jour des enregistrements (lignes) à partir d'une liste.
report_on	Permet aux utilisateurs de générer des rapports sur les tables.
report_view	Permet aux utilisateurs de générer des rapports sur les ACL de champ.
personalize_choices	Permet aux utilisateurs de configurer la table ou le champ.
data_fabric	Permet à une table d'atelier de données de référencer une table locale.

Les règles ACL d'enregistrement sont traitées dans l'ordre suivant :

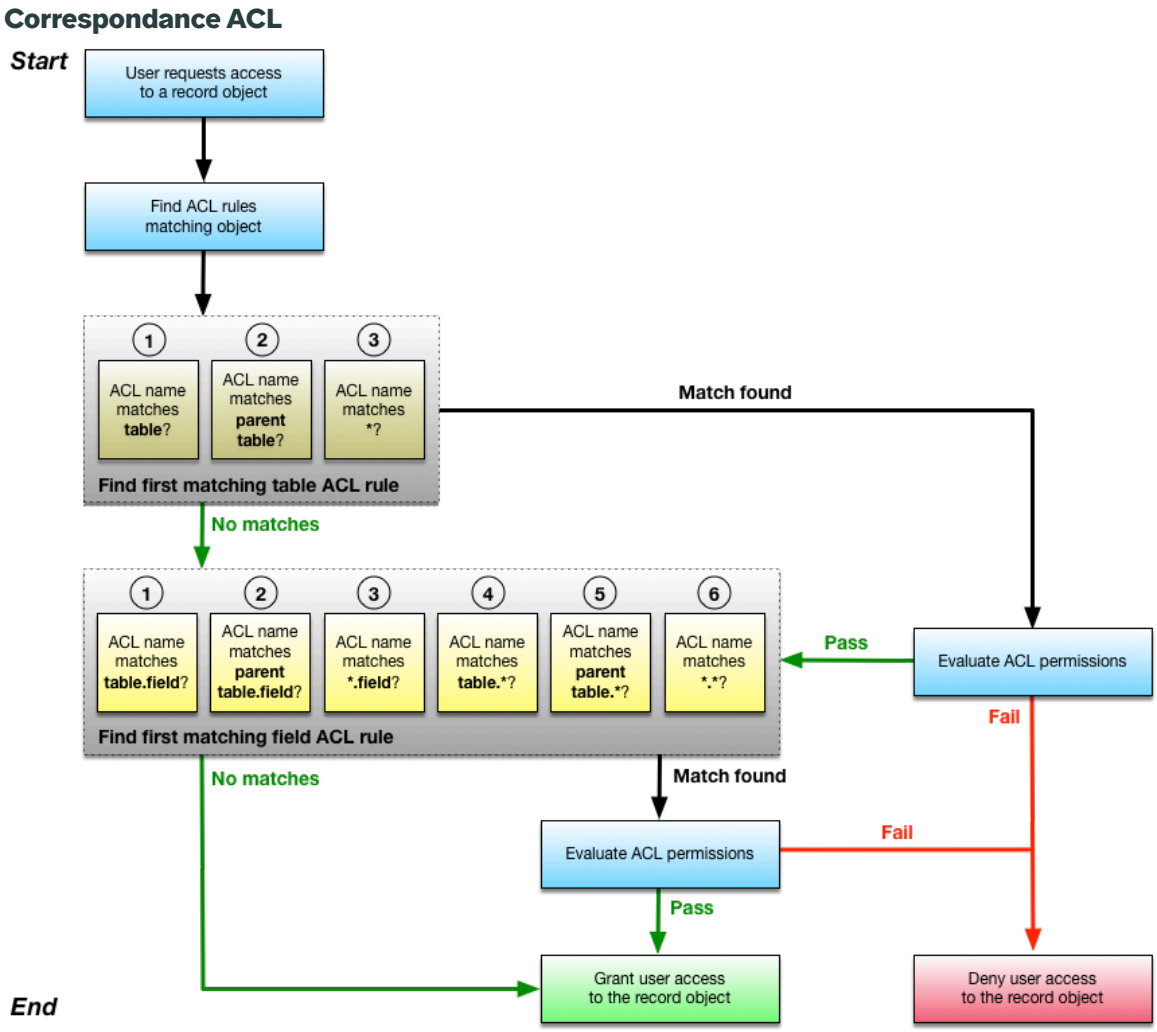
- Faites correspondre l'objet avec les règles ACL de table.
- Faites correspondre l'objet avec les règles ACL du champ.

Cet ordre de traitement garantit que les utilisateurs accèdent à des objets plus spécifiques avant d'accéder à des objets plus généraux. Un utilisateur doit respecter les règles ACL de table et de champ pour accéder à un objet d'enregistrement.

- Si un utilisateur échoue à une règle ACL de table, l'accès à tous les champs de la table lui est refusé, même s'il transmet une règle ACL de champ.
- Si un utilisateur réussit une règle ACL de table, mais échoue à une règle ACL de champ, l'utilisateur ne peut pas accéder au champ décrit par la règle ACL de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Règles ACL de processeur

Les règles ACL du processeur spécifient le processeur que vous souhaitez sécuriser. Pour obtenir la liste des processeurs disponibles, accédez à **Définition du système** > **Processeurs**.

Par défaut, une règle ACL pour EmailClientProcessor est incluse afin de restreindre le client de messagerie aux utilisateurs disposant du rôle itil.

Les règles ACL de processeur respectent la règle STAR (*) si elles ne trouvent pas d'ACL plus spécifique pour ces ressources.

Règles ACL de table

L'utilisateur doit d'abord transmettre la règle ACL de table. Étant donné que le système de base inclut des règles ACL de table STAR (*) qui correspondent à toutes les tables, l'utilisateur doit toujours transmettre au moins une règle ACL de table. Le système de base fournit des règles ACL de table supplémentaires pour contrôler l'accès à des tables spécifiques.

Les règles ACL de table sont traitées dans l'ordre suivant :

1. Correspond au nom de la table. Par exemple, incident.

2. Correspond au nom de la table parente. Par exemple, tâche.

3. Correspond à n'importe quel nom de table (*). Par exemple*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un utilisateur échoue à toutes les règles ACL de table, il ne peut accéder à aucun champ de la table. Si un utilisateur transmet une règle ACL de table, le système évalue alors les règles ACL de champ.

Règles ACL de champ

Lorsqu'un utilisateur transmet une règle ACL de table, les règles ACL de champ sont traitées dans l'ordre suivant :

1. Faites correspondre la table et le nom du champ. Par exemple, incident.number.
2. Faites correspondre la table parente et le nom du champ. Par exemple, task.number.
3. Correspond à n'importe quel nom de table (*) et de champ. Par exemple, *.numéro.
4. Faites correspondre la table et n'importe quel champ (*). Par exemple, incident.*.
5. Faire correspondre la table parente et n'importe quel champ (*). Par exemple, task.*.
6. Correspond à n'importe quelle table (*) et à n'importe quel champ (*). Par exemple*.*.

Un utilisateur doit transmettre la règle ACL de la table pour avoir accès aux champs de la table. Par exemple, l'utilisateur doit d'abord transmettre la règle ACL de table pour la table d'incidents afin d'accéder au champ **Numéro** de la table d'incidents.

La première évaluation ACL de champ réussie arrête le traitement de la règle ACL au niveau du champ. Lorsqu'un utilisateur transmet une règle ACL de champ, le système arrête la recherche d'autres règles ACL de champ correspondantes. Par exemple, si un utilisateur transmet la règle ACL de champ pour incident.number, le système arrête de rechercher d'autres règles ACL qui sécurisent le champ **Numéro** dans la table d'incidents.

L'accès aux informations de requête des données déduites est limité pour les champs protégés, empêchant ainsi le retour d'informations prédictives.

Règles ACL de la page d'interface utilisateur

Les règles ACL de la page de l'interface utilisateur spécifient la page de l'interface utilisateur à sécuriser. Pour obtenir la liste des pages de l'interface utilisateur disponibles, accédez à **Interface utilisateur du système** > **Pages de l'interface utilisateur**. Lors de la définition d'une règle ACL pour une page de l'interface utilisateur, utilisez le nom de la page dans le champ d'application complet. Par exemple, **x_myapp_mypage**.

Remarque :
Vous pouvez utiliser le caractère STAR (*) dans le champ **Nom** sur les ACL de type **ui_page** pour correspondre à toutes les pages de l'interface utilisateur.

Les règles ACL de page d'interface utilisateur respectent la règle STAR (*) si elles ne parviennent pas à trouver une ACL plus spécifique pour ces ressources. Par exemple, si vous avez une page d'interface utilisateur nommée `mysecretpage` mais que vous ne définissez pas d'ACL pour cette page d'interface utilisateur, la règle STAR (*) pour le processeur de page d'interface utilisateur est utilisée pour la vérification d'accès.

Les règles ACL peuvent sécuriser l'opération de page d'interface utilisateur suivante :

Opération	Description
Lire	Permet aux utilisateurs d'afficher la page de l'interface utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles ACL d'include de script pouvant être appelées par le client

Les règles ACL d'include de script spécifient l'include de script pouvant être appelé par le client à sécuriser. Pour obtenir la liste des includes de script disponibles, accédez à **Définition du système** > **Includes de script**. Vous pouvez personnaliser la liste pour afficher la colonne *Client appelable* .

Le système de base n'inclut aucune règle ACL pour les includes de script pouvant être appelés par le client.

Les règles ACL d'include de script pouvant être appelées par le client respectent la règle STAR (*) s'il ne trouve pas d'ACL plus spécifique pour ces ressources.

ACL de type de données

l'ACL de type de données vous permet d'écrire des règles d'ACL qui s'appliquent à tous les champs d'un type spécifique.

Les ACL de type de données offrent une approche ciblée des contrôles d'accès en limitant les champs de table en fonction du type de données. Cela permet des contraintes de sécurité plus larges que les ACL génériques (*). La syntaxe des ACL de type de données suit le format *. [(champ à restreindre)].

Les ACL de champ conventionnelles sont limitées aux identificateurs de champ de table spécifiques, à tous les champs d'une table ou à toutes les tables avec un nom de champ spécifique, en revanche, les ACL de type de données vous permettent d'appliquer la sécurité uniformément dans les champs qui partagent certaines métadonnées. Cela évite de créer des ACL supplémentaires pour appliquer la sécurité uniformément dans tous les champs.

Lors de l'implémentation des ACL de type de données, il est essentiel de valider tous les champs affectés avant et après leur ajout pour éviter des problèmes de sécurité inattendus. Reportez-vous à la section Créer une ACL de type de données pour créer votre propre ACL de type de données.

Pour examiner les ACL de type de données existantes, accédez à **Tous** > **Sécurité de système** > **Contrôles des accès** et utilisez le champ **Nom** pour rechercher les ACL commençant par *.[.

> **Remarque :**
> Scripting Governance utilise des ACL de type de données par défaut pour les restrictions de scripting, voir _ pour plus de détails.

Créer une ACL de type de données

Découvrez comment créer une ACL de type de données.

Avant de commencer
Rôle requis : admin

Procédure

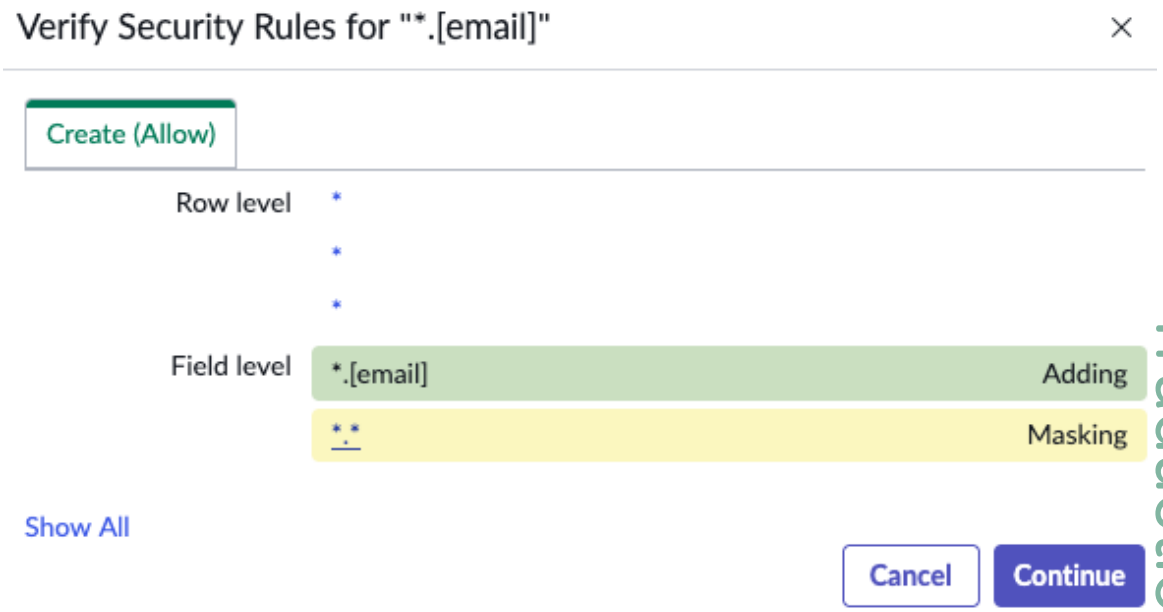
1. Accédez à la **Tous** > **Sécurité de système** > **Contrôles des accès**.
2. Sélectionnez le bouton **Nouveau** .
3. Sélectionnez l'icône Mode **de changement** près du champ **Nom**
4. Entrez votre type de données sous la forme *.[Type de données utilisateur] dans le champ **Nom** .
5. Sélectionnez un **rôle** ou un **attribut de sécurité** à associer à l'ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. **Facultatif :** Renseignez tous les détails supplémentaires dans le formulaire **Créer une ACL** . Consultez Configurer une règle ACL pour plus d'informations.
7. Sélectionnez **Soumettre**.
8. Vérifiez les règles de sécurité de l'ACL dans la fenêtre contextuelle **Vérifier les règles de sécurité** .

Exemple de règles de sécurité de vérification



Contrôle ACL des champs de fonction

Lors de l'évaluation de l'accès à un champ de fonction, en plus de vérifier l'accès au champ de fonction lui-même, le système vérifie également l'accès aux champs de contribution de la fonction. Les champs de contribution sont ceux utilisés comme arguments dans une définition de fonction donnée.

Pour plus d'informations sur les champs de fonction, voir Champ de fonction .

Dans Rome et antérieurement, le système vérifie simplement l'accès au champ de fonction lui-même (comme pour tout autre champ). Si les ACL de ce champ autorisent l'accès, l'utilisateur reçoit la valeur résultante, qu'il ait accès ou non aux champs de contribution.

Dans Yokohama et versions ultérieures, le système nécessite également l'accès à tous les champs de contribution afin de permettre l'accès au champ de fonction. Si une ou plusieurs des ACL du champ de contribution refusent l'accès, le champ de fonction refuse également l'accès.

Les seules opérations concernées par la nouvelle exigence sont la lecture et la report_view. Report_view a ses propres exigences supplémentaires.

Opération	Description
Opération de lecture	Un utilisateur a un accès en lecture à un champ de fonction uniquement si les deux conditions suivantes sont vraies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opération	Description
	• L'utilisateur a un accès en lecture au champ de fonction. • L'utilisateur a un accès en lecture à tous les champs de contribution utilisés dans la fonction.
report_view opération	Un utilisateur n'a report_view accès à un champ de fonction que si toutes les conditions suivantes sont vraies : • L'utilisateur a report_view accès au champ de fonction. • L'utilisateur a report_view accès à chacun des champs de contribution. • Il existe une ACL de lecture uniquement sans conditions et sans script, et l'utilisateur dispose de ce rôle. • L'utilisateur dispose d'un accès en lecture uniquement aux champs de contribution, de sorte que seules les ACL sans condition ni script peuvent l'autoriser.

Exemples

Donné:

- Table : salaire
- Colonnes : base, bonus, total (toutes sont des entiers dans cet exemple)
- Champ de fonction : la colonne Total est marquée comme champ de fonction, avec la définition `de fonction glidefunction :add(base, bonus).`
- Champs de contribution : base et bonus, puisqu'ils sont utilisés dans la définition de la fonction
- Rôles : salary_admin, bonus_admin

Exemple 1 : Tous les champs autorisent l'accès

ACL	Résultat
Total, Base, Bonus : lu et report_view pour les salary_admin de rôles, sans conditions ni scripts	Un utilisateur disposant du rôle salary_admin se voit accorder un accès en lecture et report_view à Total parce qu'il dispose du rôle requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple 2 : Le champ de contribution refuse l'accès en lecture

ACL	Résultat
• total, de base : lecture et report_view pour les salary_admin de rôles, sans conditions ni scripts • Bonus : report_view pour le rôle salary_admin, sans conditions ni scripts • Bonus : lecture pour les bonus_admin de rôle, sans conditions ni scripts	Un utilisateur disposant du rôle salary_admin se voit refuser l'accès en lecture et report_view au total, car la prime refuse l'accès en lecture à son rôle.

Exemple 3 : l'ACL du champ de contribution a un script

ACL	Résultat
• total, de base : lecture et report_view pour les salary_admin de rôles, sans conditions ni scripts • Bonus : report_view pour les bonus_admin de rôles, sans conditions ni scripts • Bonus : lire pour le rôle salary_admin, avec un script (notez que ce qu'il y a dans le script n'a pas d'importance, seulement qu'il est là)	Un utilisateur disposant du rôle salary_admin bénéficie d'un accès en lecture sur Total, car il dispose du rôle requis pour tous les champs. Mais le même utilisateur avec le salary_admin se voit refuser l report_view accès, car l'ACL de lecture avec le script refuse l'accès par défaut pour ce cas, même s'il a le rôle requis.

Démarrage rapide de la sécurité - Module d'extension des règles ACL

Le module d'extension de niveau de contrôle d'accès de démarrage rapide de la sécurité (règles ACL) est installé automatiquement sur toutes les nouvelles instances. Utilisez ce module d'extension pour sécuriser rapidement plusieurs tables système et accélérer le processus de lancement de la production pour votre organisation.

Ce module d'extension n'est pas destiné aux instances existantes, car il peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production. Si un administrateur souhaite fortement installer ce module d'extension sur une instance existante, vous devez d'abord le tester minutieusement dans une instance de test. Cela permet de vérifier la compatibilité avec l'implémentation actuelle de l'organisation.

Si un administrateur est intéressé par les nouvelles règles ACL fournies par ce module d'extension, il peut en créer manuellement une ou plusieurs dans une instance existante, en utilisant la liste des ACL comme guide.

Les ACL suivantes sont incluses dans ce module d'extension. Sélectionnez l'icône dans une ligne d'en-tête pour trier cette colonne par ordre croissant ou décroissant. La clé de l'opération est la suivante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- R = lecture
- W = écriture
- D=supprimer
- C=créer

Nom	Opération	Description
cmdb_ci	WCD	Actif ou rôle itil requis pour écrire/créer/supprimer des enregistrements d'éléments de configuration
cmn_department	Naine blanche	user_admin rôle requis pour écrire/supprimer des enregistrements de département
cmn_location	TOILETTE	user_admin rôle requis pour écrire/créer des enregistrements d'emplacement
core_company	Naine blanche	user_admin rôle requis pour écrire/supprimer des enregistrements de la société
kb_knowledge	créer	rôle de la base de connaissances requis pour créer des enregistrements de la base de connaissances
ldap_ou_config	RWCD	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements de définition LDAP OU
ldap_server_config	RWCD	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements du serveur LDAP
process_guide	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de guide de processus
process_step	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements d'étapes de processus
sc_category	créer	catalog_admin rôle requis pour créer des enregistrements de catégorie de Catalogue de services
sc_category	supprimer	catalog_admin rôle requis pour supprimer des enregistrements de catégorie de Catalogue de services
sc_category	écrire	catalog_admin rôle requis pour écrire dans des enregistrements de catégorie de Catalogue de services
sc_cat_item	écrire	catalog_admin rôle requis pour écrire dans des enregistrements d'éléments de catalogue
sc_cat_item	supprimer	catalog_admin rôle requis pour supprimer des enregistrements d'éléments de catalogue
sc_cat_item	créer	catalog_admin rôle requis pour créer des enregistrements d'éléments de catalogue
sysevent_email_action	Lire	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail (à des fins d'abonnement)
sysevent_register	RWCD	Rôle administrateur requis pour lire/écrire/créer/supprimer des enregistrements de registre des événements
sysevent_script_action	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements d'action de script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
syslog	RWCD	administrateur requis pour lire/écrire/créer/supprimer les enregistrements d'entrée de journal
sysrule	RWCD	administrateur tenu de lire/écrire/créer/supprimer les enregistrements de règles (notifications par e-mail, actions sur e-mail entrant, règles d'approbation, etc.)
sysrule	Lire	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail pour (notifications basées sur l'abonnement)
sys_app_application	WCD	administrateur requis pour écrire/créer/supprimer les enregistrements d'application
sys_app_category	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de catégorie d'application
sys_app_module	WCD	administrateur requis pour écrire/créer/supprimer les enregistrements du module
sys_audit	RWCD	administrateur requis pour lire/écrire/créer/supprimer les enregistrements d'audit
sys_dictionary	RWC	personalize_dictionary rôle requis pour lire/écrire/créer des enregistrements de dictionnaire
sys_dictionary.*	Lire	personalize_dictionary rôle peut lire les champs du dictionnaire
sys_documentation	supprimer	Le rôle « personalize_dictionary » est requis pour supprimer des enregistrements d'étiquette de champ.
sys_documentation	créer	Le rôle « personalize_dictionary » est requis pour créer des enregistrements d'étiquette de champ.
sys_documentation	écrire	Le Rôle « personalize_dictionary » est requis pour écrire dans des enregistrements d'étiquette de champ.
sys_gauge	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de jauge
sys_gauge_count	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de nombre de jauges
sys_group_has_role	Lire	Rôle itil requis pour afficher les enregistrements de rôle de groupe
sys_home	WCD	itil_admin rôle requis pour écrire/créer/supprimer des enregistrements de section de page d'accueil
sys_installation_exit	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer les enregistrements de sortie d'installation
sys_job	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de tâches sys
sys_nav_link	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de lien de navigation
sys_perspective	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de liste de menu
sys_portal	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements du portail
sys_portal_page	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de la page d'accueil

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_portal_preferences	RWCD	rôle administrateur requis pour lire/écrire/créer/supprimer les enregistrements des préférences du portail
sys_processor	TOILETTE	Le rôle administrateur est requis pour écrire/créer des enregistrements de processeur
sys_properties	TOILETTE	Le rôle administrateur est requis pour écrire/créer des enregistrements de propriétés système
sys_properties_category	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de catégories de propriétés
sys_report	supprimer	rôles qui peuvent supprimer des enregistrements de rapports (ne restreint pas la suppression via l'interface utilisateur de rapport)
sys_report	écrire	rôles qui peuvent écrire dans les enregistrements de rapports (ne restreint pas la modification via l'interface utilisateur du rapport)
sys_report	Lire	Les utilisateurs peuvent lire leurs propres enregistrements de rapports, ceux de leur groupe et les enregistrements GLOBAUX (n'affecte pas l'affichage via l'interface utilisateur du rapport)
sys_report	Lire	rôles qui peuvent lire les enregistrements de rapports (ne restreint pas l'affichage via l'interface utilisateur du rapport)
sys_reportroles	Lire	Le rôle administrateur est requis pour lire les enregistrements de rôles de rapport
sys_script	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de règles métier
sys_script_ajax	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de script AJAX
sys_script_client	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de script client
sys_script_include	WCD	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements Script Include
sys_security_acl	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements de contrôle d'accès
sys_security_acl_role	créer	Le rôle administrateur est requis pour créer des enregistrements de rôles d'accès
sys_security_acl_role	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de rôles d'accès
sys_security_acl_role	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements des rôles d'accès
sys_security_operation	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'opérations de sécurité
sys_security_operation	créer	Le rôle administrateur est requis pour créer des enregistrements d'opérations de sécurité
sys_security_operation	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements Security Operations
sys_security_operation	query_range	
sys_security_operation		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_security_type	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements de type de sécurité
sys_security_type	créer	Le rôle administrateur est requis pour créer des enregistrements de type de sécurité
sys_security_type	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de type de sécurité
sys_status	créer	Le rôle administrateur est requis pour créer des enregistrements d'état du système
sys_status	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'état du système
sys_status	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements d'état du système
sys_template	écrire	template_editor rôle requis pour écrire dans des enregistrements de modèles
sys_template	créer	emplate_editor rôle requis pour créer des enregistrements de modèle
sys_template	supprimer	template_editor rôle requis pour supprimer des enregistrements de modèle
sys_template	Lire	template_editor rôle requis pour lire les enregistrements des rôles de modèle
sys_ui_action	créer	Le rôle administrateur est requis pour créer des enregistrements d'actions d'interface utilisateur
sys_ui_action	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'action d'interface utilisateur
sys_ui_action	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements d'actions d'interface utilisateur
sys_ui_action_view	écrire	Le rôle administrateur est requis pour écrire dans la vue de l'interface utilisateur Enregistrements d'action
sys_ui_action_view	créer	Le rôle administrateur est requis pour créer des enregistrements d'action de vue de l'interface utilisateur
sys_ui_action_view	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'action de vue de l'interface utilisateur
sys_ui_policy	créer	Le rôle administrateur est requis pour créer des enregistrements de politique d'interface utilisateur
sys_ui_policy	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de politique d'interface utilisateur
sys_ui_policy	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements de politique d'interface utilisateur
sys_ui_policy_action	créer	Le rôle administrateur est requis pour créer des enregistrements d'actions de politique d'interface utilisateur
sys_ui_policy_action	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'actions de politique d'interface utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_ui_policy_action	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements d'actions de politique d'interface utilisateur
sys_ui_script	écrire	Le rôle administrateur est requis pour écrire dans les enregistrements de script de l'interface utilisateur
sys_ui_script	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de script d'interface utilisateur
sys_ui_script	créer	Le rôle administrateur est requis pour créer des enregistrements de script d'interface utilisateur
sys_user	écrire	Les utilisateurs n'ayant aucun rôle ne peuvent pas mettre à jour d'autre enregistrement utilisateur que le leur
sys_user_grmember	supprimer	user_admin rôle requis pour supprimer des enregistrements de membres du groupe
sys_user_grmember	écrire	user_admin rôle requis pour écrire dans les enregistrements des membres du groupe
sys_user_group	créer	Seuls ITIL et supérieur peuvent créer des enregistrements de groupe
sys_user_group	écrire	Seuls ITIL et supérieur peuvent écrire dans les enregistrements de groupe
sys_user_has_role	Lire	Le rôle itil est requis pour afficher les enregistrements de rôle d'utilisateur
sys_user_role	créer	Le rôle administrateur est requis pour créer des enregistrements de rôles
sys_user_role	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de rôles
sys_user_role	écrire	Le rôle administrateur est requis pour écrire dans des enregistrements de rôles
sys_user_role_contains	Lire	Le rôle itil est requis pour voir les enregistrements de rôles contenus
sys_user_role_contains	écrire	Le rôle administrateur est requis pour écrire dans des enregistrements de rôles contenus
sys_user_token	RWCD	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de jeton de l'utilisateur

Traduction automatique

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) [Mis à jour dans Centre de sécurité 1.3] Paramètres de la sécurisation renforcée de la sécurité de l'instance.

Configurer une règle ACL

Configurez une règle de liste de contrôle d'accès (ACL) personnalisée pour sécuriser l'accès à de nouveaux objets ou pour modifier le comportement de sécurité par défaut.

Avant de commencer
Rôle requis : security_admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Pour créer des règles ACL, vous devez élever les privilèges au rôle security_admin.

Pour les tables qui se trouvent dans un champ d'application différent de l'enregistrement de règle ACL, les types de règles sont limités. Pour les tables principales du périmètre permettant de dériver le périmètre et d'exécuter les ACL incluses dans le périmètre, définissez la *glide.enforce_security_scope.<scope_name>* propriété sur **vrai**. Cela garantit que les ACL du champ d'application global ne correspondent pas lorsque des ACL spécifiques au champ d'application sont créées dans la table pertinente. Par exemple, lors de la sécurisation des données dans des tables d'application partagées dans le périmètre global, telles que les tables sys_attachment ou sys_question_answer.

Procédure

1. Rôles à privilèges élevés au rôle security_admin.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. Cliquez sur **Nouveau**.

   Conseil :
   Lors de la création d'une nouvelle ACL, il est utile d'examiner le ACL refuser, sauf.

4. Renseignez le formulaire.

Champs de contrôle d'accès

Champ	Description
Type	Sélectionnez le type d'objet sécurisé par cette règle ACL. Le type d'objet détermine le nom de l'objet et les opérations disponibles. Ce champ passe en lecture seule après la création de la règle ACL. Si vous souhaitez modifier le type, vous devez supprimer l'ACL et en créer une nouvelle avec le type correct.
Opération	Sélectionnez l'opération que cette règle ACL sécurise. Chaque type d'objet a sa propre liste d'opérations. Une règle ACL ne peut sécuriser qu'une seule opération. Pour sécuriser plusieurs opérations, créez une règle ACL distincte pour chacune d'elles. Si vous créez une règle pour une opération report_view, reportez-vous également Report_view access control à la section .
Type de décision	Sélectionnez le type de décision de l'ACL. **Autoriser si** autorise l'accès en cas d'évaluation réussie. **Refuser sauf si** l'accès est refusé, sauf si l'évaluation est réussie. Consultez la section ACL refuser, sauf pour plus d'informations.
Remplacement administrateur	Cochez cette case pour que les utilisateurs disposant du rôle administrateur passent automatiquement la vérification des autorisations pour cette règle ACL. Les utilisateurs administrateurs réussissent, quelles que soient les restrictions de script ou de rôle qui s'appliquent. Toutefois, le rôle **personne** , que seul le ServiceNow personnel peut affecter, prime sur l'option de remplacement administrateur. Si une ACL est affectée au rôle **personne** , les utilisateurs administrateurs ne peuvent pas accéder à la ressource, même lorsque l'option **Remplacements administrateur** est sélectionnée. Voir Rôles système de base . Décochez cette case si les administrateurs doivent satisfaire aux autorisations définies dans cette règle ACL pour accéder à l'objet sécurisé. Étant donné que les administrateurs réussissent toujours les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	vérifications de rôle (voir la description du champ **Exige un rôle**), utilisez le générateur de conditions ou le champ **Script** pour créer une vérification des autorisations que les administrateurs doivent vérifier.
Politique de protection	Sélectionnez cette option pour définir la politique de protection sur l'ACL
Nom	Entrez le nom de l'objet sécurisé, soit le nom de l'enregistrement, soit les noms de table et de champ. Plus le nom est précis, plus la règle ACL est spécifique. Vous pouvez utiliser le caractère générique astérisque (*) à la place d'un nom d'enregistrement, de table ou de champ pour sélectionner tous les objets qui correspondent à un type d'enregistrement, à toutes les tables ou à tous les champs. Vous ne pouvez pas combiner un caractère générique et une recherche de texte. Par exemple, inc* n'est pas un nom de règle ACL valide, mais incident.* et *.number sont des noms de règle ACL valides. **Remarque :** Cliquez sur le triangle bleu pour entrer manuellement le nom de l'enregistrement ou les noms de table et de champ de l'objet à sécuriser. Utilisez cette option pour sécuriser un objet qui n'apparaît pas dans la liste déroulante.
Description	Entrez une description de l'objet ou des autorisations que cette règle ACL sécurise.
Actif	Cochez cette case pour appliquer cette règle ACL.
Avancés	Cochez cette case pour afficher les champs **de condition avancée** . Voir l'étape 6.

5. **Facultatif :** Pour réduire le champ d'application de l'ACL, renseignez les champs **Conditions** si nécessaire.

Demande un rôle	Utilisez cette liste pour spécifier les rôles qu'un utilisateur doit avoir pour accéder à l'objet. Si vous répertoriez plusieurs rôles, un utilisateur disposant de l'un des rôles répertoriés peut accéder à l'objet. La liste *Exige un rôle* apparaît sous forme de liste connexe. **Remarque :** Les utilisateurs disposant du rôle administrateur réussissent toujours cette vérification des autorisations, car le rôle administrateur leur accorde automatiquement tous les autres rôles.
Condition de données	Utilisez ce générateur de conditions pour sélectionner les champs et les valeurs qui doivent être vrais pour que les utilisateurs puissent accéder à l'objet. **Remarque :** Le champ Condition est sensible à la casse

6. **Facultatif :** Si la case **Avancé** est cochée, renseignez les champs Conditions **avancées** au besoin

Contrôlé par références	Applique l'ACL sur les enregistrements connexes. Reportez-vous à la rubrique Accès à l'enregistrement connexe pour en savoir plus.
Script	Entrez un script personnalisé décrivant les autorisations requises pour accéder à l'objet. Le script peut utiliser les valeurs des variables globales *actuelles* et *précédentes* dans les règles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

métier ainsi que les propriétés système. Le script doit générer une réponse vrai ou faux de l'une des deux façons suivantes :

- Renvoyer un jeu de variables de *réponse* à une valeur vrai ou faux
- Évaluer à vrai ou faux

Dans les deux cas, les utilisateurs n'accèdent à l'objet que lorsque le script est évalué comme vrai et qu'ils remplissent toutes les conditions de la règle ACL. Les conditions et le script doivent être définis sur vrai pour qu'un utilisateur puisse accéder à l'objet.

S'il y a un script dans le champ Script. Ce script s'exécute même si le champ n'est pas affiché sur le formulaire.

Remarque :
Si l'élément évalué se trouve dans une liste connexe, **l'élément actuel** pointe vers l'élément sur lequel se trouve la liste connexe, et non vers l'élément actuel auquel l'ACL est destinée. Toutefois, si l'élément pour lequel vous évaluez l'ACL n'est pas dans une liste connexe, **l'élément actuel** pointe vers l'élément réel.

---

7. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

ACL refuser, sauf

En savoir plus sur les ACL refuser-exigible.

Les ACL refuser-sauf sont évaluées avec une approche « refuser sauf si ». L'ACL définit les utilisateurs qui ne seront PAS refusés. En d'autres termes, l'accès sera refusé à l'utilisateur **si** les exigences relatives au rôle, à la condition et au script ne sont pas remplies.

Important :
Les ACL refuser-sauf seront prioritaires sur les ACL Autoriser si dans l'évaluation d'ACL, car elles seront évaluées en premier.

Une ACL refuser-sauf produit deux résultats

Résultat de l'évaluation	Résultat
Succès	Les rôles, les conditions de données, les attributs de sécurité et les exigences de script définis sont remplis. L'ACL procède à une évaluation plus approfondie **Important :** Les ACL Allow-If doivent toujours accorder l'accès au sujet pour pouvoir accéder à la ressource.
Échec	L'ACL Refuser sauf est marquée comme défaillante et l'accès sera refusé.

Voici un exemple expliqué d'ACL refuser-sauf :

- ACL a les rôles sn_hr_core.manager et itil
- La condition a actif = vrai
- script a answer = gs.isLoggedIn() ;

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'accès est refusé à l'utilisateur sauf si les trois exigences de cette ACL sont satisfaites. Pour que cette ACL refuser-sauf passe, l'utilisateur doit avoir le rôle sn_hr_core.manager ou itil , accéder à un enregistrement dont le champ actif = vrai doit être validé et être connecté. L'ACL Refuser sauf échouera si l'une des trois exigences n'est pas remplie.

Autoriser l'ACL

En savoir plus sur Autoriser les ACL (listes de contrôle d'accès).

Les ACL d'autorisation sont conçues pour accorder l'accès aux ressources par défaut, sauf si une règle spécifique le refuse. C'est le contraire d'un modèle « Refuser-Sauf si ».

ACL de requêtes

Les ACL de requête vous permettent de définir un contrôle d'accès plus granulaire en définissant explicitement qui peut interroger les données.

Qu'est-ce qu'une ACL de requête

L'opération des ACL de requête est définie sur `query_range` ou sur `query_match`. Les ACL de requête permettent un contrôle plus spécifique des requêtes utilisateur, en limitant ou en activant l'accès en fonction de leur configuration. Les ACL de requête sont des outils puissants contre les attaques de requête aveugle, où un attaquant interroge aveuglément les données pour extraire des informations des résultats, même lorsqu'il ne peut pas voir les valeurs.

Quand utiliser une ACL de requête

Lorsqu'une colonne contient des valeurs sensibles et autorise un accès partiel/conditionnel aux données, une ACL de requête doit être envisagée et mise en œuvre si nécessaire en fonction de la sensibilité des données. Lorsqu'il existe un accès partiel/conditionnel aux lignes et à leurs colonnes dans les tables, en particulier lorsque cet accès n'est pas appliqué par des filtres de données, des ACL de requête doivent être implémentées si nécessaire en fonction de la sensibilité des données.

Remarque :
Envisagez des ACL de requête lorsque certains utilisateurs ont accès à certaines lignes ou colonnes et pas à d'autres.

Example: Contrôle de la requête de paie

Je peux voir une ligne dans le tableau de salaire avec mon salaire, mais il n'y a aucune raison pour que je puisse émettre des requêtes de plage pour interroger des utilisateurs dont le salaire est contenu dans 2 limites. Une `query_range` ACL sur le salaire m'empêcherait d'émettre cette requête.

Example: Contrôle de requête RH

Je peux voir tout hr_profiles, mais je ne peux voir le SSN que par moi-même. Je n'ai pas à interroger le NSS, et les ACL de requête doivent m'empêcher d'exécuter des requêtes sur le NSS d'autres profils RH pour essayer d'extraire des mappages de NSS.

Comportement de l'ACL de requête

Les ACL de requête utilisent des opérations `query_match` et `query_range` pour un comportement d'interrogation de table sécurisé et granulaire. Leurs comportements sont décrits ci-dessous :

`query_match`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

query_match est composé de : EQUALS, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISEMPTYSTRING, ISEMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL. query_match est faite des « opérateurs sûrs », dans le sens où ils sont construits pour récupérer des enregistrements spécifiques et ne peuvent pas être exploités pour en renvoyer d'autres.

Résultat de l'évaluation	Résultat
Succès	L'utilisateur peut soumettre des requêtes de correspondance
Échec	L'utilisateur ne sera pas en mesure de soumettre des requêtes de correspondance : • ÉGALE • NOT_EQUALS • DANS • NOT_IN • SAMEAS • NSAMEAS • RIEN • CHAÎNE D'OBJETS ISEMPTYSTRING • ISEMPTY • ISNOTEMPTY • ISNULL • ISNOTNULL

query_range

query_range est composé de tous les autres (STARTS_WITH, CONTAINS, >=, <= etc.) qui sont plus dangereux car ils permettent aux utilisateurs d'interroger plus d'enregistrements en ajustant les valeurs limites.

Résultat de l'évaluation	Résultat
Succès	L'utilisateur peut soumettre des requêtes de plage et le tri est illimité
Échec	L'utilisateur ne sera pas en mesure de soumettre des requêtes de plage avec (STARTS_WITH, CONTAINS, >=, <=, etc. Le tri par colonne est restreint

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

Les ACL de requête (query_match et query_range) sont par défaut une ACL star.star qui délègue l'accès en lecture. Cela signifie que lorsque les ACL sont appliquées aux requêtes, si aucune ACL de requête n'a été créée, l'accès en lecture à la colonne est évalué ; si des ACL de requête sont définies, elles remplacent le comportement par défaut.

Enregistrements sécurisés dans une liste incorporée

Pour appliquer la sécurité aux enregistrements des listes incorporées, limitez la modification et la suppression des enregistrements des listes incorporées à des rôles spécifiques.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Contrôle d'accès (ACL)**.
2. Ouvrez l'enregistrement **Écrire** ou **Supprimer** pour la table appropriée.
3. Dans la section Exige un rôle du formulaire, ajoutez les rôles qui ont une autorisation d'écriture ou de suppression pour cette table.
4. Enregistrez les changements.
   Lorsque les enregistrements de la table associée apparaissent dans une liste incorporée, les options de modification et de suppression ne sont disponibles que pour les utilisateurs disposant des rôles spécifiés.

Accès à l'enregistrement connexe

L'accès aux enregistrements connexes permet un contrôle cohérent sur les enregistrements auxquels les utilisateurs peuvent accéder entre les tables connexes.

Détails de l'accès à l'enregistrement connexe

L'accès à l'enregistrement connexe vous permet de configurer l'accès à l'enregistrement connexe, en déterminant si l'ACL de la table parente connexe doit être appliquée aux données dont l'accès est autorisé à partir de l'ACL. Prenons le cas d'utilisation suivant : un utilisateur a accès à un enregistrement via ACL, puis l'accès à l'enregistrement connexe permet aux utilisateurs d'accéder à tous les autres enregistrements qui lui sont associés, via une référence ou une relation bidirectionnelle.

Gestionnaire de sécurité contextuelle

Le gestionnaire de sécurité contextuelle protège vos données en contrôlant l'autorisation de lecture, d'écriture, de création et de suppression.

Avantages clés

Le gestionnaire de sécurité contextuelle connaît la hiérarchie de la table système, ce qui vous permet de créer des règles de sécurité spécifiques pour un champ en fonction de l'emplacement d'affichage dans la hiérarchie. Les avantages du gestionnaire de sécurité contextuelle comprennent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Sécurité contextuelle** : sécurisez un enregistrement en fonction du contenu de l'enregistrement.
- **Sécurité hiérarchique** : appliquez des règles de sécurité à n'importe quel niveau de la hiérarchie des objets.

Sécurisation des champs et des tables

Avec l'ancien Simple Security Manager, vous pouvez sécuriser les champs et les tables en ajoutant des rôles à l'entrée de dictionnaire appropriée. Avec Contextual Security Manager, ces rôles de dictionnaire ne sont plus testés. Au lieu de cela, le système recherche les règles ACL sur les champs et les tables.

⚠ Avertissement :
Après avoir installé le gestionnaire de sécurité contextuelle, vous devez sécuriser les champs et les tables à l'aide de règles ACL. Même si vous configurez le formulaire , mettez en page le formulaire dictionnaire et ajoutez des rôles à une entrée de dictionnaire, aucun changement de droits ne se produit.

Sécurité contextuelle et rôles

Vous pouvez accorder des rôles aux utilisateurs ou aux groupes. Cependant, après l'installation du gestionnaire de sécurité contextuelle **, le champ** rôles de l'enregistrement utilisateur n'est plus vérifié et n'apparaît plus sur vos formulaires d'utilisateur et de groupe. Au lieu de cela, vous devez ajouter des rôles à la liste connexe Rôles plutôt qu'à l'enregistrement d'utilisateur ou de groupe.

Les applications et les modules contiennent des listes des rôles requis pour les afficher. Par exemple, pour afficher l'application System Definition, le rôle administrateur est requis. Les droits de sécurité pour les applications et les modules sont toujours définis à l'aide de tableaux de rôles.

Les éléments de catalogue et les variables de catalogue contiennent des listes des rôles requis pour les afficher. Les droits de sécurité pour les éléments de catalogue et les variables de catalogue sont toujours définis via ces tableaux de rôles.

Sous le Gestionnaire de sécurité contextuelle, un groupe hérite toujours automatiquement de tout rôle qui lui est accordé lorsque le marqueur d'héritage du rôle est défini sur *vrai*.

Activation du gestionnaire de sécurité contextuelle

Le gestionnaire de sécurité contextuelle est actif dans le système de base. S'il existe de nombreuses entrées en double dans la table Rôles d'utilisateur, vous devrez peut-être effectuer une mise à niveau vers Sécurité contextuelle : gestion des rôles V2 pour éliminer les rôles en double. Les modules d'extension incluent :

Sécurité contextuelle : gestion des rôles [com.glide.role_management]

Fournit une fonctionnalité de sécurité contextuelle. Ce module d'extension est automatiquement installé.

Sécurité contextuelle : gestion des rôles V2 [com.glide.role_management.inh_count]

Empêche les entrées en double causées par les rôles hérités dans la table Rôles d'utilisateur [sys_user_has_role]. Ce module d'extension est automatiquement installé sur les nouvelles instances et peut être activé pour les mises à niveau. Le module d'extension Sécurité contextuelle : améliorations de la gestion des rôles est une version précédente de ce module d'extension. Le module d'extension Améliorations de la gestion des rôles n'inclut pas le script RoleManagementVerify(). Ce script renvoie une liste des changements qu'une mise à niveau effectuera, ce qui vous permet de surveiller les changements apportés par le module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Après avoir activé Gestion des rôles V2, vous devez définir la propriété système glide.role_management.v2.audit_roles pour permettre à la table Rôles d'audit de créer des enregistrements d'audit liés aux rôles d'utilisateur. Pour en savoir plus sur la définition de cette propriété et sur la table Rôles d'audit, voir :

- Activer l'audit des rôles avec la sécurité contextuelle : gestion des rôles V2.
- Paramètres de sécurisation renforcée dans les paramètres de renforcement de la sécurité de l'instance.
- Rôles d'utilisateur d'audit

Empêcher les entrées en double avec Sécurité contextuelle : gestion des rôles V2

Les rôles hérités d'autres rôles sont ajoutés en tant qu'entrées individuelles dans la table Rôles d'utilisateur [sys_user_has_role], ce qui peut entraîner des entrées en double pour un rôle. Sécurité contextuelle : Gestion des rôles V2 élimine ces entrées en double et empêche les doublons futurs.

Éliminer les entrées en double grâce au nombre d'héritages

Sécurité contextuelle : Gestion des rôles V2 utilise la colonne Nombre d'héritages (inh_count) pour suivre le nombre de fois où un rôle est hérité d'un autre rôle ou groupe. Dans la table Rôles d'utilisateur [sys_user_has_role], un utilisateur ne peut hériter d'un rôle spécifique qu'une seule fois, ce qui élimine les entrées en double. La colonne Nombre d'héritages (inh_count) est en lecture seule et calcule le nombre de fois que l'utilisateur hérite d'un rôle.

Changements d'activation

Sécurité contextuelle : Gestion des rôles V2 est automatiquement installée sur les nouvelles instances et peut être activée pour les mises à niveau. Lorsqu'elle est activée, Sécurité contextuelle : gestion des rôles V2 remplace à la fois Sécurité contextuelle et Sécurité contextuelle : améliorations de la gestion des rôles.

Lorsque Sécurité contextuelle : gestion des rôles V2 est activée, les colonnes suivantes sont obsolètes, mais restent dans la table Rôles d'utilisateur pour des raisons de rétrocompatibilité :

- granted_by (utilisé uniquement par la délégation de rôle)
- included_in_role
- included_in_role_instance

Avertissement :
Si ces colonnes sont utilisées dans des scripts personnalisés sur votre instance, n'effectuez pas de mise à niveau vers Gestion des rôles V2.

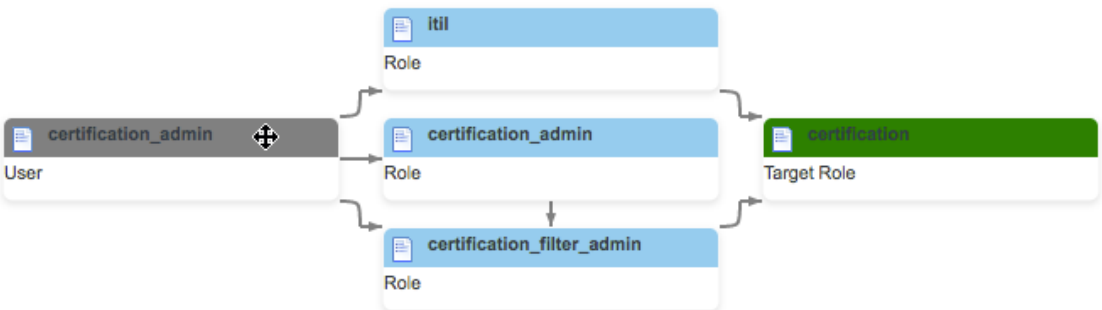
Visualiser l'héritage des rôles via la carte d'héritage de rôle

La carte d'héritage de rôle affiche une représentation visuelle des rôles hérités. Vous pouvez utiliser cette carte pour comprendre les rôles représentés dans la colonne Nombre d'héritages (inh_count). Pour afficher la carte d'héritage de rôle, configurez la table Rôles d'utilisateur [sys_user_has_role] pour afficher la colonne Carte d'héritage de rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Carte d'héritage de rôle



Remarque :
La mise à jour simultanée de l'affectation de groupe ou de rôle peut entraîner un nombre d'héritages incorrect. Vous devez activer la propriété glide.security.inh_count_patcher.enabled pour obtenir le nombre exact d'héritages.

Mise à niveau vers la sécurité contextuelle : gestion des rôles V2

Sécurité contextuelle : Gestion des rôles V2 est automatiquement installé sur les nouvelles instances. Vous pouvez effectuer une mise à niveau de Sécurité contextuelle : gestion des rôles vers Sécurité contextuelle : gestion des rôles V2 pour éliminer les rôles en double dans la table Rôles d'utilisateur et empêcher les futurs doublons.

Avant de commencer

Rôle requis : admin, security_admin

Vous devez disposer du rôle admin et Accéder à un rôle privilégié obtenir le rôle de security_admin effectif.

Remarque :
Avant d'effectuer une mise à niveau vers Sécurité contextuelle : Rôle : Gestion V2, vous devez activer la table Rôles d'audit pour créer des enregistrements d'audit liés aux rôles d'utilisateur. Pour en savoir plus sur la définition de la propriété système requise, reportez-vous à la section Activer l'audit des rôles avec la sécurité contextuelle : gestion des rôles V2.

Pourquoi et quand exécuter cette tâche

Cette procédure décrit comment mettre à niveau votre rôle de sécurité contextuelle et comment activer les modules d'extension connexes décrits dans le tableau suivant.

Modules d'extension pour la sécurité contextuelle : gestion des rôles v2

Module d'extension	Description
Sécurité contextuelle : gestion des rôles V2 [com.glide.role_management.inh_count]	Empêche les entrées en double dans la table Rôles d'utilisateur [sys_user_has_role]. Le rôle security_admin ou un utilisateur avec des privilèges élevés est requis pour activer le module d'extension ou contacter Service client et assistance.
Sécurité contextuelle : REST API Gestion des rôles V2 [com.glide.role_management.inh_count.rest_api]	Active la fonctionnalité d'API pour la gestion des rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de passer de Contextual Security : Role Management à Contextual Security : Role Management V2, testez les résultats d'une mise à niveau en exécutant le script. Le script renvoie une liste des modifications qu'une mise à niveau effectuera. Si les changements sont acceptables, installez le module d'extension Sécurité contextuelle : gestion des rôles V2. Si les changements ne sont pas acceptables, n'installez pas le module d'extension Sécurité contextuelle : gestion des rôles V2. Vous pouvez également effectuer la mise à niveau, puis apporter manuellement les modifications nécessaires.

Procédure

1. Testez l'impact d'une mise à niveau avant la mise à niveau en exécutant le script suivant.

   a. Accédez à la **Définition du système** > **Scripts - Arrière-plan**.

   b. Exécutez le script suivant dans le champ d'application global.

   ```
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   Pour les tables sys_user_has_role volumineuses, l'exécution peut prendre plusieurs heures. Ne modifiez pas et n'ajoutez pas de rôles d'utilisateur pendant cette période.
   Exemple de résultat basé sur des données de test :

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
   *** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED:
    api_analytics_read,pa_viewer,rest_api_explorer,a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
   *** Script: Number of inherited-role records in sys_user_has role, current: 260, after
    re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
   ```

   c. Évaluez les résultats du script pour déterminer si les changements proposés sont acceptables.

2. Activez le module d'extension Sécurité contextuelle : gestion des rôles V2.

   Important :
   Le rôle security_admin ou un utilisateur avec des privilèges élevés est requis pour activer le module d'extension ou contacter Service client et assistance.

   a. Accédez à la **Définition du système** > **Modules d'extension**.

   b. Recherchez et cliquez sur le nom du module d'extension.

   c. Dans le formulaire Module d'extension système, examinez les détails du module d'extension, puis cliquez sur le lien connexe **Activer/mettre à niveau** .

   d. Cliquer sur **Activer**.

Résultats

Après l'activation de Gestion des rôles V2, les changements décrits dans le résultat du script sont mis en œuvre. La colonne Nombre d'héritages (inh_count) de la table Rôles d'utilisateur est en lecture seule et reflète automatiquement le nombre de fois où l'utilisateur hérite d'un rôle.

Activer l'audit des rôles avec la sécurité contextuelle : gestion des rôles V2

Définissez une propriété système pour permettre à la table Rôles d'audit de créer des enregistrements d'audit liés aux rôles d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Lorsqu'elle est activée, la table Rôles d'audit [sys_audit_role] conserve les changements apportés aux enregistrements utilisateur. Pour plus d'informations sur les audits de rôles, consultez Rôles d'utilisateur d'audit . Si le module d'extension Sécurité contextuelle : gestion des rôles V2 [com.glide.role_management.inh_count] est installé, vous devez définir une propriété système sur **vrai** pour activer l'audit des rôles.

Procédure

1. Accédez à la table Propriétés système [sys_properties].
2. Ajoutez la `glide.role_management.v2.audit_roles` propriété système et définissez-la sur **vrai**.

   Si le module d'extension Sécurité contextuelle : gestion des rôles V2 [com.glide.role_management.inh_count] est installé, la définition de cette propriété sur **vrai** permet à la table Rôles d'audit [sys_audit_role] de créer des enregistrements lorsque les rôles d'utilisateur changent.

Revérifier la soumission du formulaire

Lorsque le système détermine qu'un champ particulier (tel que task.number) ne doit pas être écrit par l'utilisateur actuel, il affiche ce champ en mode lecture seule, ce qui explique pourquoi le champ numéro n'est pas accessible en écriture sur la plupart des incidents.

Si vous configurez le système pour vérifier à deux fois les valeurs de tous les champs entrants pour vérifier l'écriture, le système applique le même ensemble de règles de sécurité au segment entrant d'une transaction. Lorsque vous soumettez un incident, par exemple, le système vérifie à deux reprises si le champ Numéro peut être écrit avant de publier des modifications.

Si vous demandez au système de ne pas revérifier les transactions entrantes, le système vous permet d'écrire dans un champ nominalement en lecture seule s'il s'agit de la transaction renvoyée par le client. Dans de nombreux déploiements, il s'agit en fait d'un comportement souhaitable si, par exemple, vous utilisez des scripts clients pour définir des champs nominalement en lecture seule en réponse à des sélections d'utilisateurs dans d'autres champs accessibles en écriture.

Propriété	Emplacement	Par défaut
Revérifiez la sécurité des transactions entrantes durant la soumission du formulaire (les droits sont toujours vérifiés lors de la création d'un formulaire)	**Propriétés système** > **Sécurité**	Désactivé (pas de double vérification)

Propriété de refus par défaut

La propriété de refus par défaut (glide.sm.default_mode) contrôle le comportement par défaut du gestionnaire de sécurité lorsque les seules règles ACL correspondantes sont les règles ACL de la table à caractère générique.

Un ensemble de règles ACL de table à caractère générique est disponible pour les opérations basées sur les enregistrements les plus courantes : lecture, écriture, création

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et suppression. Un nombre important d'ACL permettant d'accéder aux tables système en fonction des rôles est également disponible. Par exemple, il existe des ACL qui sys_script accordent l'accès au rôle business_rule_admin, car ce rôle est documenté comme étant capable de gérer les règles métier.

Utilisez la propriété glide.sm.default_mode pour refuser ou autoriser ces opérations sur toutes les tables :

- **Refuser l'accès** : les règles ACL de la table à caractère générique restreignent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf si l'utilisateur a le rôle administrateur ou répond aux exigences d'une autre règle ACL de table. Les autres opérations, telles que report_on et personalize_choices, ne sont pas affectées par ce paramètre.
- **Autoriser l'accès** : les règles ACL de table à caractère générique autorisent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf s'il existe des règles ACL de table spécifiques en place pour restreindre de telles opérations.

Vous ne pouvez pas réinitialiser glide.sm.default_mode sur **Autoriser l'accès** une fois qu'il a été défini sur **Refuser l'accès**.

Remarque :
Par défaut, les règles ACL de la table à caractère générique sont les seules règles ACL qui vérifient la valeur de la propriété glide.sm.default_mode . Si vous souhaitez contrôler d'autres opérations avec ce paramètre, créez vos propres règles ACL pour vérifier cette valeur de propriété.

Pour en savoir plus sur cette propriété, consultez Refuser par défaut en cas d'ACL vides [Mis à jour dans Centre de sécurité 1.3] Paramètres de renforcement de la sécurité de l'instance.

Configuration avancée de l'ACL

En plus de créer de nouvelles ACL ou de modifier celles qui existent déjà, vous pouvez configurer d'autres aspects de la fonctionnalité des ACL.

Refuser les règles ACL

Refuser sauf

Règles ACL de requête

Tâche	Description
Appliquer les conditions de script ACL aux champs de référence	Activez une propriété pour permettre aux conditions de script de s'appliquer aux champs de référence si vous souhaitez contrôler l'accès aux données qu'un champ de référence affiche sur un formulaire ou une liste. L'activation de cette option pourrait avoir un impact sur les performances de votre instance.
Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)	Appliquez des ACL aux appels d'API `GlideAjax` afin que le système interroge uniquement les données auxquelles l'utilisateur actuellement connecté a le droit d'accéder.
Évaluer le contournement	Forcer l'évaluation ACL pour les remplacements administrateur au niveau de l'accès. Par défaut, les utilisateurs disposant du rôle administrateur passent automatiquement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
administrateur au niveau de l'accès	la vérification des autorisations pour cette règle ACL lorsque l'option Remplacements administrateur est sélectionnée sur le formulaire Règles ACL.
Utiliser des outils de débogage et de dépannage d'ACL	Utilisez des outils tels que l'observateur d'ACL, le débogage au niveau des champs et accédez aux messages de sortie des règles ACL pour vous aider à dépanner et à déboguer les ACL.

Fournir l'accès à une table aux utilisateurs externes

Pour permettre aux utilisateurs ayant seulement le rôle snc_external d'accéder à la vue de liste d'une table, vous devez créer une série d'ACL.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accéder à un rôle privilégié.
2. Créez une règle ACL avec les paramètres suivants :
   - **Type** : ui_page
   - **Opération** : lecture
   - **Nom** : {table_name}_list
   - **Rôle requis** : snc_external
3. Sur les ACL de **lecture** par défaut pour la table, ajoutez **snc_external** dans la liste des Rôles requis. Créez l'ACL s'il n'existe pas encore.
4. Utilisez les paramètres suivants pour créer un autre ACL :
   - **Type** : ui_page
   - **Opération** : lecture
   - **Nom** : {table_name}
   - **Rôle requis** : snc_external
5. Utilisez les paramètres suivants pour créer un autre ACL afin de fournir à l'utilisateur l'accès en écriture à un champ dans la table :
   - **Type** : enregistrement
   - **Opération** : créer
   - **Nom** : {table_name} {column_name}
   - **Rôle requis** : snc_external

   Répétez cette étape pour chaque champ auquel vous souhaitez donner l'accès en écriture à l'utilisateur. Utilisez un astérisque * à la place du nom de la colonne pour donner accès à tous les champs à la fois.

Appliquer les conditions de script ACL aux champs de référence

Utilisez la propriété système pour activer les *glide.sys_reference_row_check* conditions scriptées pour les champs de référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le comportement par défaut vise à améliorer les performances de l'instance. Si vous souhaitez activer les conditions de script pour les champs de référence, ajoutez la propriété système suivante.

Remarque :
Pour plus d'informations sur la création de propriétés système, reportez-vous à la section Add a system property .

Propriété système

Propriété	Description
glide.sys_vérification_ligne_référence_	Contrôle si les conditions de script des règles de contrôle d'accès s'appliquent aux champs de référence d'une table. • Type : true | false • Valeur par défaut : **faux** • Emplacement : ajouter une propriété système à la table Propriétés système [sys_properties]

Remarque :
Si la propriété système n'est pas présente ou a été définie sur faux, les conditions de script pour les `glide.sys_reference_row_check` règles de contrôle d'accès ne sont pas appliquées. Cela signifie qu'une ACL contenant des conditions de script passera sa vérification avec succès tant que les autres critères d'ACL sont remplis (tels que les exigences du rôle).

Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)

Utilisez une propriété système pour valider la règle de liste de contrôle d'accès (ACL) lorsque vous accédez aux enregistrements côté serveur (par exemple, les tables) à l'aide d'API GlideAjax à l'intérieur d'un script client.

Si vous choisissez d'appliquer des listes de contrôle d'accès (ACL) aux appels `d'API GlideAjax` , vous ne pouvez interroger que les données auxquelles l'utilisateur actuellement connecté a des droits d'accès. Par exemple, si l'utilisateur est connecté en tant qu'utilisateur ESS qui n'a pas le droit de lire la table `cmn_location` , tout appel d'API `GlideAjax` par l'utilisateur échouera.

Si l'API s'exécute ServiceNow AI Platform sans vérification des appels GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

Utilisez GlideRecordSecure lors de l'interrogation des données pour garantir le niveau de sécurité le plus élevé. GlideRecord s'appuie sur l'application des ACL par le biais de configurations, tandis que GlideRecordSecure applique des contrôles de sécurité plus stricts. GlideRecordSecure offre une solution plus sécurisée et prête à l'emploi pour le traitement des données sensibles.

Remarque :
Définir cette propriété dans **Propriétés système** > **Sécurité**.

Propriété	Par défaut
Appliquez des ACL de sécurité standard aux appels `AJAXGlideRecord`	Vérification ACL appliquée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Les sys_class_name, sys_id et sys_domain sont ignorés pour les vérifications ACL.

Pour en savoir plus sur cette propriété, consultez Exiger la vérification de l'ACL AJAXGlideRecord [Mis à jour dans Centre de sécurité 1.3] Paramètres de renforcement de la sécurité de l'instance.

Évaluer le contournement administrateur au niveau de l'accès

Si vous souhaitez forcer l'évaluation d'ACL pour les remplacements d'administrateur au niveau de l'accès, vous pouvez ajouter une propriété système.

Avant de commencer

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Les ACL sont évaluées de façon cumulative. S'il existe un certain nombre d'ACL sur un champ donné et que l'option **Remplacements administrateur** est **définie sur faux** (non sélectionné), les remplacements administrateur effectifs pour toutes les ACL sont considérés comme **faux**. Les administrateurs ne peuvent donc même pas transmettre l'ACL où le remplacement doit être effectué.

Procédure

Ajoutez la propriété suivante à la table des propriétés système :

Propriété	Description
glide.security.admin.override.accessterm	Évalue la condition de remplacement administrateur au niveau des conditions d'accès. • Type : true | false • Valeur par défaut : **true** pour les nouvelles instances, **false** pour les mises à niveau • Emplacement : ajouter à la table Propriétés *[sys_properties]* système **Remarque :** Si la propriété n'est pas définie sur l'instance, la valeur est évaluée comme faux.

Outils de débogage ACL

Des messages de sortie de règle ACL de débogage et d'accès au niveau du champ sont disponibles pour vous aider à dépanner et à déboguer les ACL. L'observateur de configuration ACL vous permet de savoir quelles ACL connexes existent lorsque vous en modifiez une.

Débogage au niveau du champ

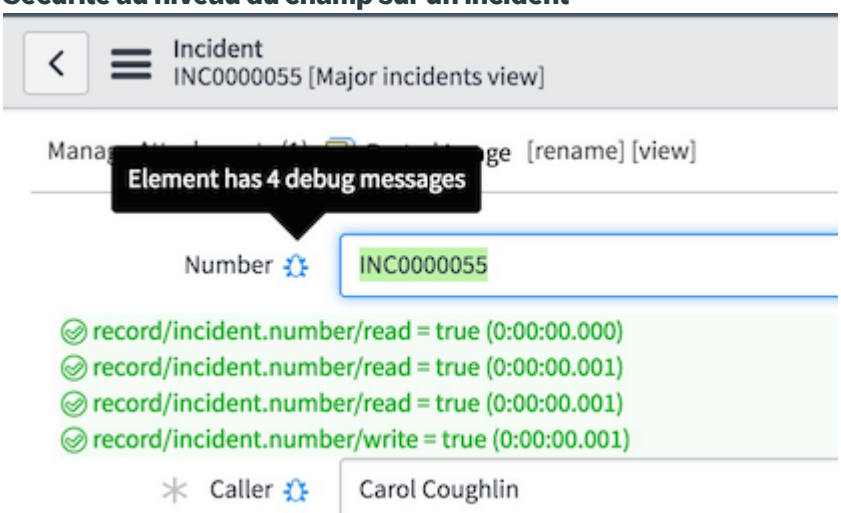
Lorsque le débogage est activé, une petite icône de bogue ( ) apparaît en regard de chaque champ avec une règle ACL. Cliquez sur l'icône pour afficher les règles ACL qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

s'appliquent au champ et aux résultats de l'évaluation. Activer le débogage en accédant à **Sécurité de système** > **Débogage** > **Déboguer les règles de sécurité**.

Sécurité au niveau du champ sur un incident



Après avoir activé le débogage d'ACL, vous pouvez emprunter l'identité d'un autre utilisateur pour voir quelles règles ACL l'utilisateur transmet et échoue. Lorsque vous empruntez l'identité d'un utilisateur, vous ne pouvez voir que ce que cet utilisateur est autorisé à voir. Par exemple, vous ne pouvez pas afficher un enregistrement qu'une ACL empêche l'utilisateur de voir. Pour faciliter le débogage, l'accès en lecture seule à certaines tables liées aux ACL est activé par défaut, même en empruntant l'identité d'un utilisateur qui ne dispose pas d'un accès en lecture aux tables. Pour modifier cette fonctionnalité, définissez la propriété suivante sur **faux**.

Pour activer le débogage d'une règle ACL, accédez à **Sécurité de système** > **Déboguer les règles de sécurité**.

Propriété système	Description	Paramètre par défaut
glide.security.access_acl	Autorise l'accès en lecture aux tables suivantes en empruntant l'identité d'un utilisateur : sys_security_acl, sys_security_operation, sys_security_type et sys_user_role. Par conséquent, l'utilisateur dont l'identité a emprunté l'identité peut lire des données que l'utilisateur dont l'identité a été empruntée ne peut pas lire.	vrai **Remarque :** Lorsque la propriété est définie sur false, l'utilisateur dont l'identité a été empruntée peut être empêché de lire les données liées aux ACL. Dans ce cas, une deuxième session connectée en tant qu'administrateur ou security_admin peut être nécessaire pour déboguer les ACL.

Messages de sortie de règle ACL

Le débogage d'ACL affiche les messages de sortie de la règle ACL au bas de chaque liste et formulaire. Le message de sortie affiche les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de message	Description
HEURE	Temps total utilisé pour traiter cette règle ACL.
CHEMIN D'ACCÈS	Informations qui identifient de manière unique chaque règle ACL au format suivant : <Type de règle ACL>/<Nom de règle ACL>/<Opération>.
CONTEXTE	Objet évalué par la règle ACL.
RC	Code de retour de la règle ACL. Une valeur réelle passe la règle ACL. Une valeur erronée ne respecte pas la règle ACL.
RÈGLE	Bref résumé des processeurs et des scripts, suivi des résultats ACL pour chaque évaluation ACL au niveau de la table et du champ. La plupart des évaluations ACL montrent un résultat global de réussite ou d'échec suivi d'une répartition des résultats pour chaque type de critères ACL : • iAccessHandler : vérification interne du système à l'aide du code source masqué sur la plateforme. Il s'agit d'un contrôle de sécurité du système que vous ne pouvez pas modifier. Le gestionnaire d'accès peut accorder ou refuser l'accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées. Vous ne pouvez en aucun cas modifier les vérifications du gestionnaire d'accès. Par exemple, une implémentation IAccessHandler est utilisée pour les contrôles d'accès sur les ressources d'application et ne peut pas être modifiée. Cette option est disponible à partir de la Istanbul version. • Rôles : vérification que l'utilisateur dispose du rôle approprié. • Condition : vérification que l'utilisateur a réussi la condition spécifiée dans la règle ACL (le cas échéant). • Script : vérification que l'utilisateur a transmis le script spécifié sur la règle ACL (le cas échéant).

Les icônes qui s'affichent montrent comment l'ACL a été évaluée :

Icône	Description
Une coche verte ( )	Indique que la table ou le champ a satisfait aux critères.
Icône X rouge ( )	Indique que la table ou le champ n'a pas réussi.
Une icône de cercle gris vide ( )	Indique que l'évaluation ACL n'a pas eu besoin d'être effectuée.
Une coche bleue, un x ou un cercle vide	Indique que l'ACL a été prise à partir d'un résultat mis en cache d'une vérification précédente de l'ACL. Les icônes signifient la même chose que ci-dessus.

Vous pouvez effectuer ces actions sur la sortie de débogage d'ACL :

- Activez ou désactivez ces cases à cocher en haut de la sortie de débogage :
  - **Règles de sécurité** : affichez ou masquez les résultats des vérifications d'ACL.
  - **Autres** : afficher ou masquer d'autres avertissements ou messages.

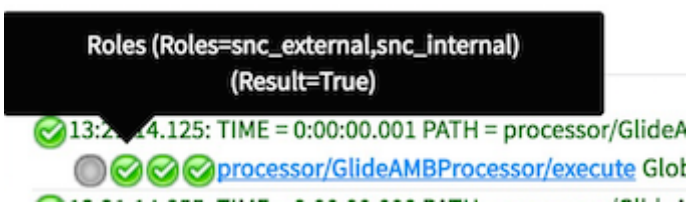
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur le nom de l'ACL en regard de l'un des messages de sortie pour ouvrir cet enregistrement ACL.



- Placez le curseur sur l'une des icônes des quatre vérifications ACL pour afficher plus d'informations.



Référence de dépannage ACL

Une liste des erreurs courantes des règles ACL et de leurs solutions.

Activez le débogage pour faciliter la résolution d'un problème.

Dépannage

Erreur ou symptôme	Solution
Vous ne pouvez pas accéder aux enregistrements à partir d'une table personnalisée.	Créez une règle ACL de table pour la table personnalisée accordant aux utilisateurs l'accès à la table. Sans règle ACL de table explicite, les utilisateurs doivent transmettre les autorisations de la règle ACL de caractère générique de table (*), qui restreint par défaut l'accès aux administrateurs uniquement. Activez le débogage et déterminez les règles ACL qui sont évaluées pour la table personnalisée.
Vous créez une règle ACL personnalisée qui ne fonctionne pas correctement.	Les problèmes les plus probables sont qu'une autre règle prévaut sur votre règle personnalisée dans l'ordre de traitement ou que l'utilisateur ne répond pas à toutes les exigences d'autorisation pour le type d'objet. Activez le débogage et vérifiez que la règle ACL est en cours d'évaluation.
Votre règle ACL de champ ne fonctionne pas correctement.	Il existe probablement une règle ACL de table que l'utilisateur n'a pas respectée. Activez le débogage et déterminez quelles règles ACL sont évaluées pour le champ. Vérifiez qu'il n'y a pas de règle ACL de table en conflit ou de règle ACL de champ en double.
Votre règle ACL de table ne fonctionne pas correctement.	Il existe soit une règle ACL plus haut dans l'ordre de traitement, soit une règle ACL de table en double interfère avec la règle ACL de la table. Activez le débogage et déterminez quelles règles ACL sont évaluées pour la table.
Vous pouvez voir un champ dans une liste, mais pas dans le formulaire.	Il est possible que les conditions ou le script de la règle ACL soient déclenchés dans la liste, mais pas dans le formulaire. Activez le débogage et déterminez quand les règles ACL sont évaluées comme vraies. Mettez à jour les conditions ou le script pour avoir le même comportement sur la liste et le formulaire.
Vous recevez un message d'erreur lorsque vous essayez d'exécuter un	Il existe une règle ACL pour le processeur ou l'include de script appelable par le client que l'utilisateur n'a pas respectée. Si l'utilisateur doit avoir accès à l'objet, activez le débogage et déterminez quelles règles ACL sont évaluées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Erreur ou symptôme	Solution
processeur ou un include de script pouvant être appelé par le client.	pour le processeur ou l'include de script. Mettez à jour la règle ACL ou les rôles d'utilisateur selon les besoins pour accéder à l'objet.

Observateur de configuration ACL

L'observateur de configuration ACL vous permet de savoir quelles ACL connexes existent dans une table lorsque vous insérez, mettez à jour ou supprimez une ACL de la même table.

L'observateur de configuration ACL est une fenêtre d'intercepteur qui s'affiche chaque fois que vous apportez des modifications importantes à la table Contrôle d'accès [sys_security_acl]. Il affiche une fenêtre de synthèse des règles de sécurité dans laquelle vous pouvez voir les ACL associées à celle que vous modifiez. Vous ne pouvez modifier aucune ACL à partir de la fenêtre des règles de sécurité. Pour apporter des modifications, fermez la fenêtre de l'observateur et accédez à ces ACL.

L'observateur de configuration ACL n'apparaît pas dans les situations suivantes :

- Si vous enregistrez ou mettez à jour un enregistrement ACL sans réellement apporter de modifications.
- Si vous effectuez des mises à jour mineures (pas une insertion ou une suppression), telles que la mise à jour des scripts, des conditions et l'option admin-overrides.
- Si l'enregistrement ACL n'est pas actif.

Fenêtre Règles de sécurité ACL

L'observateur de configuration affiche le plan d'exécution de l'ACL. Le plan d'exécution s'affiche dans la fenêtre contextuelle des règles de sécurité. Vous pouvez afficher ce type d'informations :

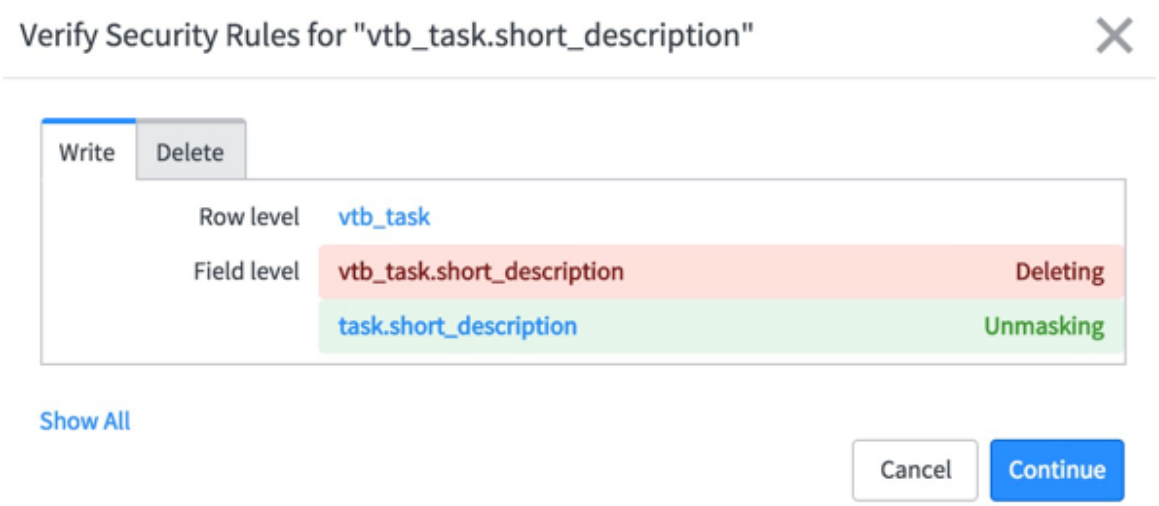
Éléments de la fenêtre de configuration ACL

Élément	Description
Surlignage rouge	ACL supprimée ou désactivée.
surlignage bleu	ACL modifiée.
Surlignage vert	ACL ajoutée ou active.
Masqué	ACL qui était efficace jusqu'à ce que vous effectuiez un changement.
Démasqué	Un ACL qui vient d'entrer en vigueur lorsque vous avez effectué un changement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'observateur de configuration



Afficher le plan d'exécution de l'ACL

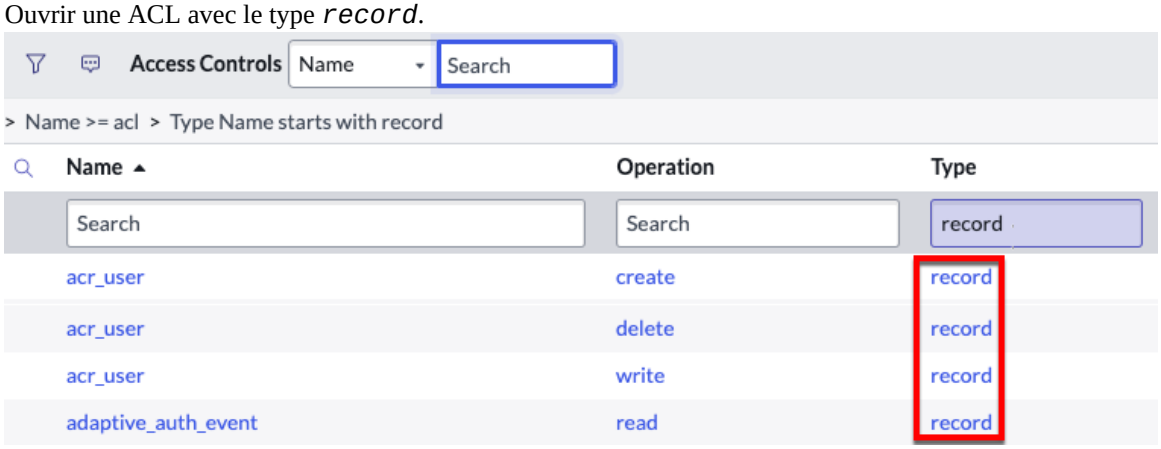
Les administrateurs peuvent voir comment les ACL sont liées les unes aux autres en affichant un plan d'exécution pour n'importe quelle ACL de l'instance.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accéder à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. Ouvrir une ACL avec le type *`record`*.

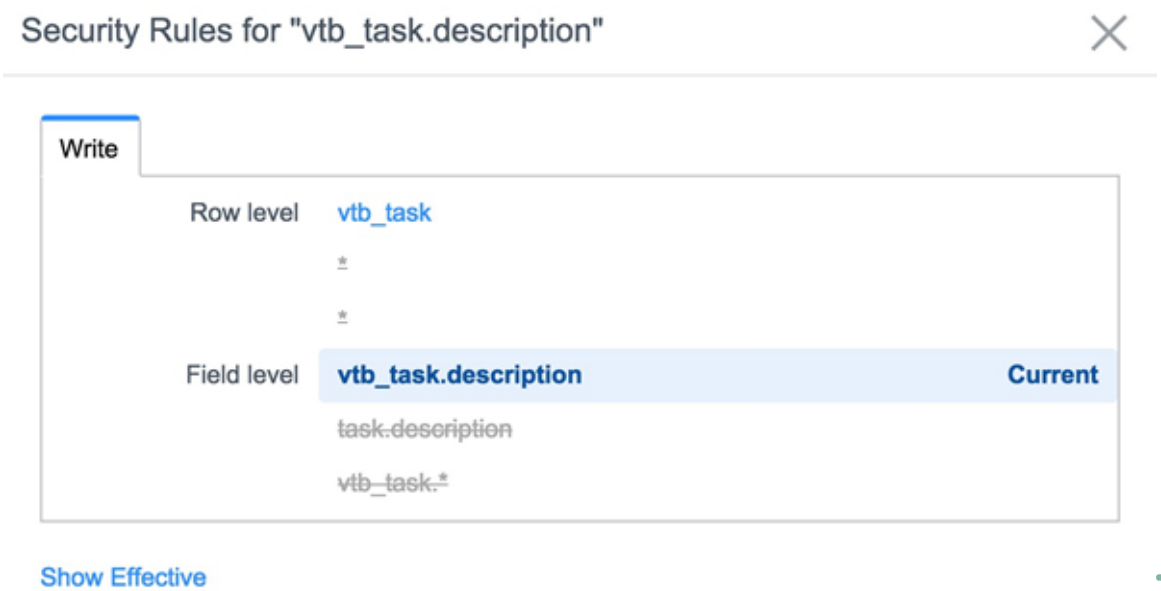


4. Cliquez sur **Afficher le plan d'exécution de l'ACL** dans la section Liens connexes.

   La fenêtre des règles de sécurité s'affiche pour l'ACL. L'exemple affiche le plan d'exécution pour « vtb_task ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Fenêtre de plan d'exécution ACL

Élément d'interface utilisateur	Description
Titre	Nom de l'ACL.
Nom d'onglet	Si l'ACL est créer, lire, écrire ou supprimer.
Niveau de ligne	ACL au niveau des lignes qui s'exécutent sur cette table.
Niveau de champ	ACL au niveau du champ qui s'exécutent uniquement sur ce champ (ou cette colonne de la table).

5. Cliquez sur **Tout afficher** pour afficher toutes les ACL associées, y compris les ACL qui sont remplacées et les ACL génériques qui s'appliquent à tous les enregistrements.
   Les ACL remplacées sont barrées par une ligne et les ACL génériques sont accompagnées d'un astérisque de caractère générique (*) pour le nom.
6. Affichez uniquement les ACL immédiates associées à celle que vous consultez et masquez les ACL dans les tables à partir desquelles la table d'ACL est étendue et les ACL génériques génériques (*) en cliquant sur **Afficher les données effectives**.

Utiliser l'observateur de configuration ACL

Utilisez l'observateur de configuration ACL après avoir atteint security_admin rôle.

Avant de commencer

Rôle requis : security_admin
Accéder à un rôle privilégié

Procédure

1. Ouvrez une ACL de type enregistrement.
2. Effectuez une action sur l'ACL, comme la modifier ou sélectionner une option dans le menu contextuel comme **Insérer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

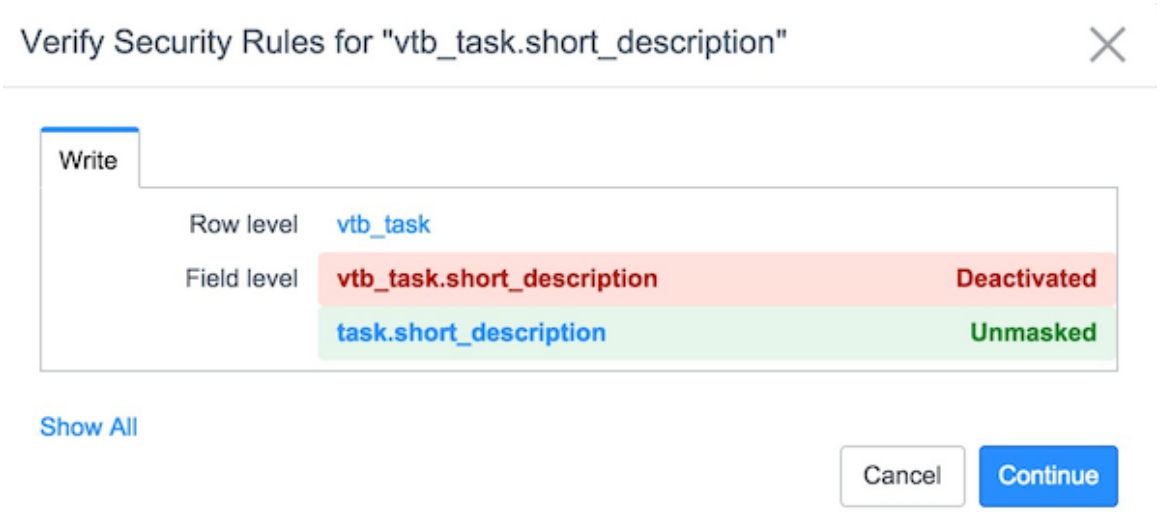
3. Si vous avez modifié des valeurs dans le formulaire Contrôle d'accès, cliquez avec le bouton droit sur l'en-tête et sélectionnez **Enregistrer** ou cliquez sur **Mettre à jour** ou **supprimer**.

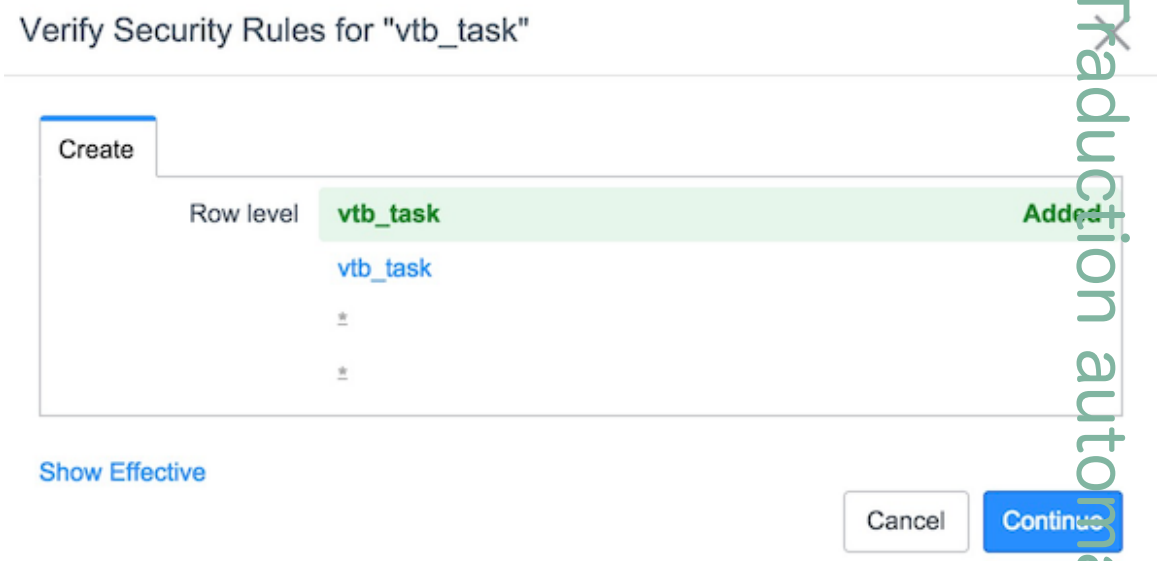
   La fenêtre Règles de sécurité s'affiche. Le système n'a pas encore effectué l'action de base de données sur l'ACL, les changements ne sont donc pas encore enregistrés.

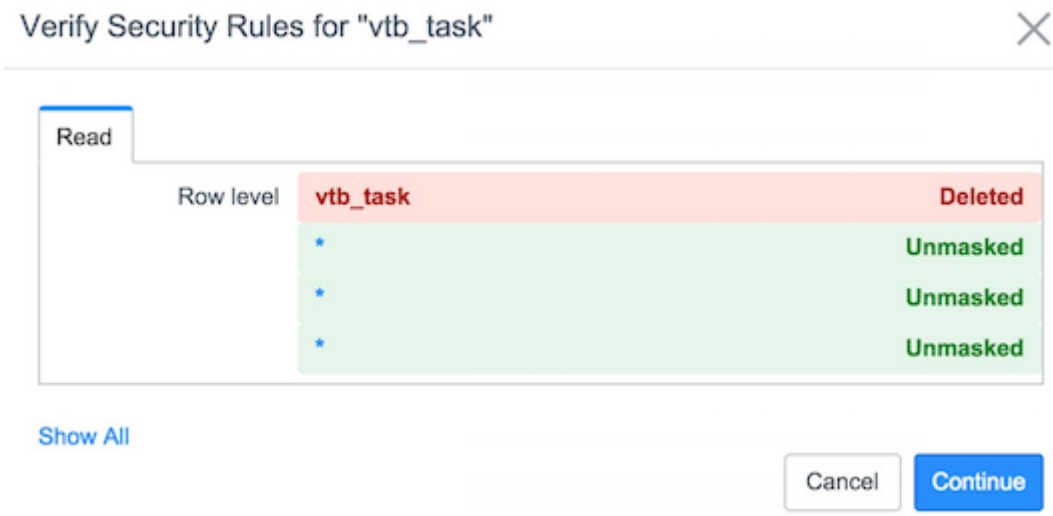
   Il s'agit d'exemples de règles de sécurité sur la table Tâche privée [vtb_task] de l'application Visual Task Board. Consultez la section Observateur de configuration ACL pour obtenir une description des éléments de cette fenêtre.

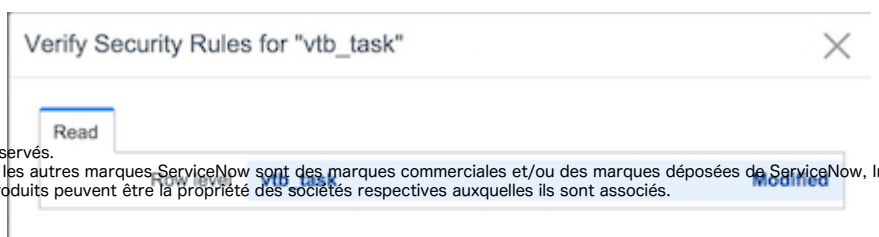
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.









Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

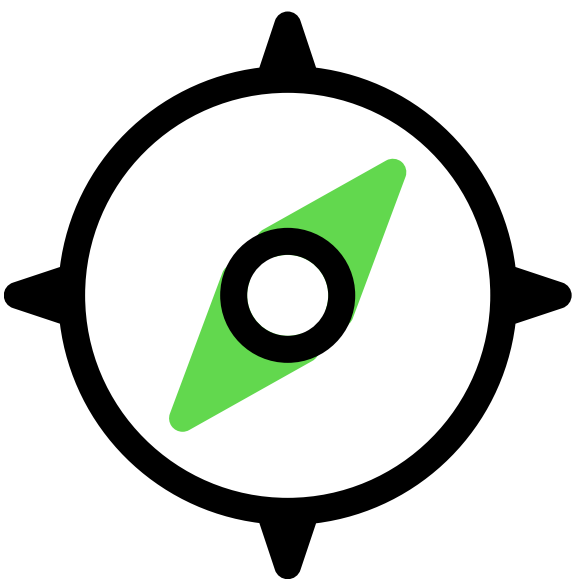
4. Comme pour le plan d’exécution, vous pouvez cliquer sur **Afficher tout** pour afficher toutes les ACL associées, y compris celles qui sont remplacées et les ACL génériques qui s’appliquent à tous les enregistrements, ou cliquer sur **Afficher effectif** pour afficher uniquement les ACL immédiates associées à celle que vous consultez.
5. Passez votre souris sur l’une des ACL pour afficher une description.

Attributs de sécurité

Les attributs de sécurité offrent une alternative flexible aux listes de contrôle d’accès.

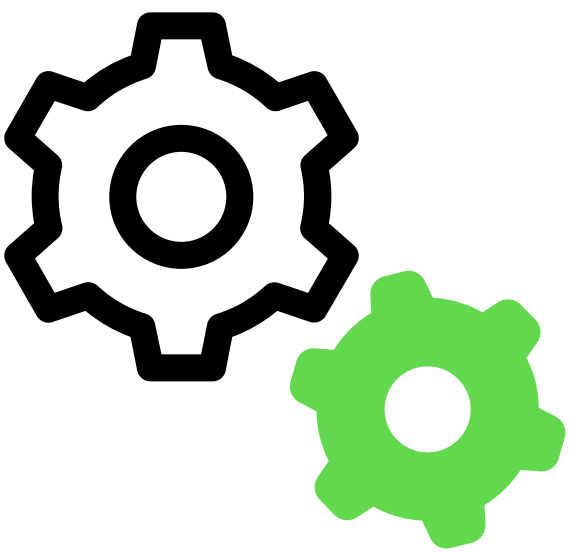
Premiers pas

Explorer les attributs de sécurité



Découvrir les notions fondamentales des attributs de sécurité

Créer des attributs de sécurité

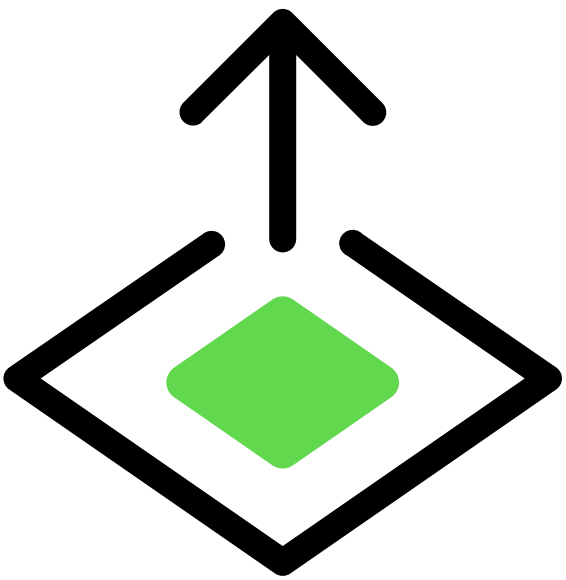


Créer de nouveaux attributs de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs de sécurité OOB (prêts à l’emploi)



Expliquer les attributs de sécurité OOB

Connexion des attributs de sécurité

Examiner la journalisation de l’attribut de sécurité

Notions fondamentales des attributs de sécurité

Un attribut de sécurité est une information hautement configurable sur un sujet ou son environnement, lorsqu’il est utilisé dans les contrôles d’accès, permet une configuration de sécurité fine de manière non complexe.

Vue d'ensemble

Les attributs de sécurité offrent une méthode alternative pour le contrôle d’accès via des définitions de rôles à la configuration des listes de contrôle d’accès (ACL) actuellement pratiquée. Les attributs de sécurité offrent plusieurs avantages aux configurations basées sur ACL :

Meilleure sécurité

L’amélioration de l’obfuscation de l’évaluation des autorisations garantit la sécurité de votre organisation.

Lisible par l’homme

Les attributs de sécurité sont conçus pour simplifier la création et la facilité d’utilisation des autorisations de sécurité.

Sécurité flexible

Créez des définitions de profil à partir de la configuration prête à l’emploi en combinaison avec des profils définis par le client.

Journalisation et audit

Les attributs de sécurité offrent un audit et une journalisation détaillés pour donner plus d’informations sur les mesures et la théorie de sécurité.

Créer des attributs de sécurité

Créez de nouveaux attributs de sécurité grâce à un guide étape par étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Sécurité de système** > **Attributs de sécurité**.
2. Dans la liste Attributs de sécurité, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Attributs de sécurité.

Champs d'attributs de sécurité

Champ	Description
Étiquette	Étiquette de l'attribut de sécurité.
Nom	Nom de l'attribut de sécurité.
Type	Type d'attribut de sécurité. ○ Composé **Remarque :** Pour plus d'informations sur les attributs de sécurité composés, voir Attributs de sécurité composés ○ entier ○ liste ○ chaîne ○ booléen (vrai/faux)
Est dynamique	Si la valeur de l'attribut de sécurité doit être réévaluée pour chaque élément
Description	Description de l'attribut de sécurité générée par l'utilisateur
Application	Champ statique, périmètre de l'application.
Table de recherche	Référencez une table externe pour l'évaluation.
Colonne de table de recherche	Référencez une colonne de table pour l'évaluation.
Script	Dériver une valeur d'un script.

Attributs de sécurité OOB (prêts à l'emploi)

Attributs de sécurité généralisés couramment utilisés Rôles prêts à l'emploi.

Vue d'ensemble

Les attributs de sécurité prêts à l'emploi sont un moyen facile de commencer à utiliser et à apprendre les options des attributs de sécurité avec une série de rôles d'attribut de sécurité préconfigurés. Les rôles d'attribut de sécurité OOB sont des rôles de contrôle d'accès couramment utilisés.

Pour créer votre propre attribut de sécurité ou développer les options d'attributs de sécurité prêts à l'emploi, consultez Attributs de sécurité composés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs de sécurité OOB

Attribut	Description
Groupe	L'utilisateur est membre d'un groupe spécifié
GroupExplicite	L'utilisateur est un membre explicite d'un groupe spécifique
HasAdminRole	L'utilisateur a le profil administrateur
Emprunt d'identité	L'identité de l'utilisateur a été empruntée
Session interactive	Session interactive en cours
Connecté	L'utilisateur est connecté et authentifié
Critères réseau	Critères réseau supplémentaires
Rôle	L'utilisateur a un rôle spécifique
Rôle explicite	L'utilisateur a un rôle spécifique explicitement défini

Attributs de sécurité pour la session client

Les attributs de sécurité suivants sont ajoutés pour la session client (module d'extension : com.glide.client_session_security_attributes) :

- [store-future: BEGIN review]**IsEmbeddedSession** : l'attribut est utilisé dans les ServiceNow composants Web intégrés.

  Remarque :
  IsEmbeddedSession est ajouté en tant qu'attribut de sécurité uniquement lorsque le module d'extension Embedded client Access (com.glide.security.client_access) est installé.

  [End]

- **IsIframeEmbeddedSession** : l'attribut est utilisé dans l'iframe intégré dans les portails tiers. Par exemple, Engagement Messenger, Client Web de l'Agent virtuel, Session incorporée...
- **IsIntegrationAsAServiceSession** : l'attribut est utilisé dans les applications de messagerie telles qu'Agent virtuel dans Teams, Agent virtuel dans Slack et Agent virtuel dans WhatApp.
- **IsIntegrationAsAUserSession** : attribut utilisé dans Utilisateur de compte d'intégration ou Utilisateur de service web.
- **Est une session Web ServiceNow** : l'attribut est utilisé dans la session Web interactive.
- **Est une session d'application mobile** : l'attribut est utilisé si la propriété **mobile_client** est vraie dans l'enregistrement **de oauth_entity** .

Remarque :
Vous devez utiliser **IsIframeEmbeddedSession**, **IsIntegrationAsAServiceSession** et **IsIntegrationAsAUserSession** uniquement lors de la configuration du type de client pour les enregistrements OAuth et SSO. Pour en savoir plus, consultez Configurer le type de client pour les enregistrements OAuth et SSO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explication du comportement non explicite et explicite

Les attributs de sécurité répondent à des besoins d'autorisation nuancés avec une évaluation explicite ou non explicite (héritée) des autorisations de rôle.

[qa: BEGIN review]

Example: Séparer l'accès aux fichiers d'un rôle IT de l'accès aux fichiers d'un rôle RH

Nous définirons un attribut de sécurité qui permet à l'administrateur de voir les fichiers RH, mais n'autorise pas l'accès aux fichiers d'administrateur. Supposons que le rôle administrateur ne soit pas défini dans le cadre du groupe RH, mais qu'il soit _____. Le **rôle** voit _____[End]

Attributs de sécurité composés

Les attributs de sécurité composés vous permettent de créer des profils d'attributs de sécurité cohérents et réutilisables en fonction des besoins de votre entreprise

Vue d'ensemble

Les attributs de sécurité composés sont définis à partir d'un ou plusieurs attributs de sécurité préexistants afin de créer une combinaison de référence unique d'attributs de sécurité pour l'évaluation des autorisations.

[qa: BEGIN review]

Comportement de l'attribut de sécurité composé

[End]

Créer un composé Attributs de sécurité

Créez un attribut de sécurité composé pour une réutilisation facile.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Sécurité de système** > **Attributs de sécurité**.
2. Dans la liste Attributs de sécurité, sélectionnez **Nouveau**.
3. Sélectionnez `Composé` dans le champ **Type** .
4. Renseignez les champs du formulaire Attributs de sécurité.

Champs d'attributs de sécurité

Champ	Description
Étiquette	Étiquette de l'attribut de sécurité.
Nom	Nom de l'attribut de sécurité.
Description	Description de l'attribut de sécurité générée par l'utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Conditions spécifiques d'attribut de sécurité utilisées pour définir l'évaluation des attributs de sécurité.
Nouveau critère	Ajoutez un ensemble supplémentaire de conditions **OU** pour l'évaluation.

Périmètre de l'attribut de sécurité

Les attributs de sécurité prennent en charge les options de définition du champ d'application.

Définition du champ d'application de l'attribut de sécurité

Le comportement inclus dans le champ d'application des attributs de sécurité est cohérent avec les comportements de définition du champ d'application de la plateforme. Les attributs de sécurité créés dans un périmètre ne sont disponibles que dans les contrôles d'accès du même périmètre.

Attributs de sécurité locaux et existants

Les attributs de sécurité existants et locaux permettent aux clients de réutiliser les ensembles de conditions d'attribut de sécurité.

Attributs locaux et existants

Le générateur de conditions d'attribut de sécurité ACL permet aux clients de spécifier si un attribut de sécurité est existant ou local.

Remarque :
Les conditions des attributs de sécurité sont définies par défaut sur local.

Un attribut de sécurité défini localement est enregistré uniquement dans l'ACL unique dans laquelle il est créé.

L'option existante permet aux utilisateurs de référencer une condition d'attributs de sécurité existante dans le générateur de conditions.

Requête de champ Rôles et restrictions

Les attributs **Rôles de requête de champ** et **Restrictions de requête de champ**vous permettent de mieux contrôler les informations disponibles pour les utilisateurs dans les tables.

Vue d'ensemble

Les attributs **Rôles de requête de champ** et **Restrictions de requête de champ** permettent un contrôle plus précis des actions que les utilisateurs peuvent effectuer sur les tables.

Rôles de requête de champ

Empêche l'interrogation des champs sensibles en fonction du rôle de l'utilisateur.

Restrictions de requête de champ

Limitez l'accès à l'enregistrement si l'accès au champ applicable est refusé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un rôle de requête de champ

Découvrez comment activer et configurer un attribut de rôle de requête de champ.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Tables**.
2. Sélectionnez une **table**.
3. Sélectionnez une **étiquette de colonne** pour afficher son entrée **de dictionnaire** .
4. Sélectionnez l'onglet **Attributs**.
5. **Conseil :**
   Si vous ne disposez pas du champ **Rôles de requête de champ** , sélectionnez **Nouveau** pour en créer un

   Sélectionnez l’attribut **Rôles de requête de champ** .
6. Entrez les rôles requis pour afficher cette colonne de table dans la **valeur**
7. Sélectionner **Mettre à jour**

Résultats
La colonne de table ne peut être interrogée que par les rôles définis dans l’attribut **Rôles de requête de champ** . Si un utilisateur sans rôles définis interroge la colonne de table, l’accès à l’opération lui sera refusé.

Configurer les restrictions de requête de champ

Apprendre à configurer une restriction de requête de champ

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Tables**.
2. Sélectionnez une **table**.
3. Sélectionnez une **étiquette de colonne** pour afficher son entrée **de dictionnaire** .
4. Sélectionnez l'onglet **Attributs**.
5. **Conseil :**
   Si vous ne disposez pas du champ **Requête de champ Restreindre l’accès aux enregistrements** , sélectionnez **Nouveau** pour en créer un

   Sélectionnez l’attribut **Requête de champ Restreindre l’accès aux enregistrements** .
6. Entrez `la valeur vrai` dans le champ **Valeur** pour restreindre l’accès aux enregistrements aux seuls utilisateurs autorisés à consulter le champ, sinon saisissez `la valeur faux`.
7. Sélectionner **Mettre à jour**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
La colonne de table limitera les résultats de toutes les requêtes. Les utilisateurs restreints sont informés du nombre de résultats renvoyés par une requête, mais aucune autre information.

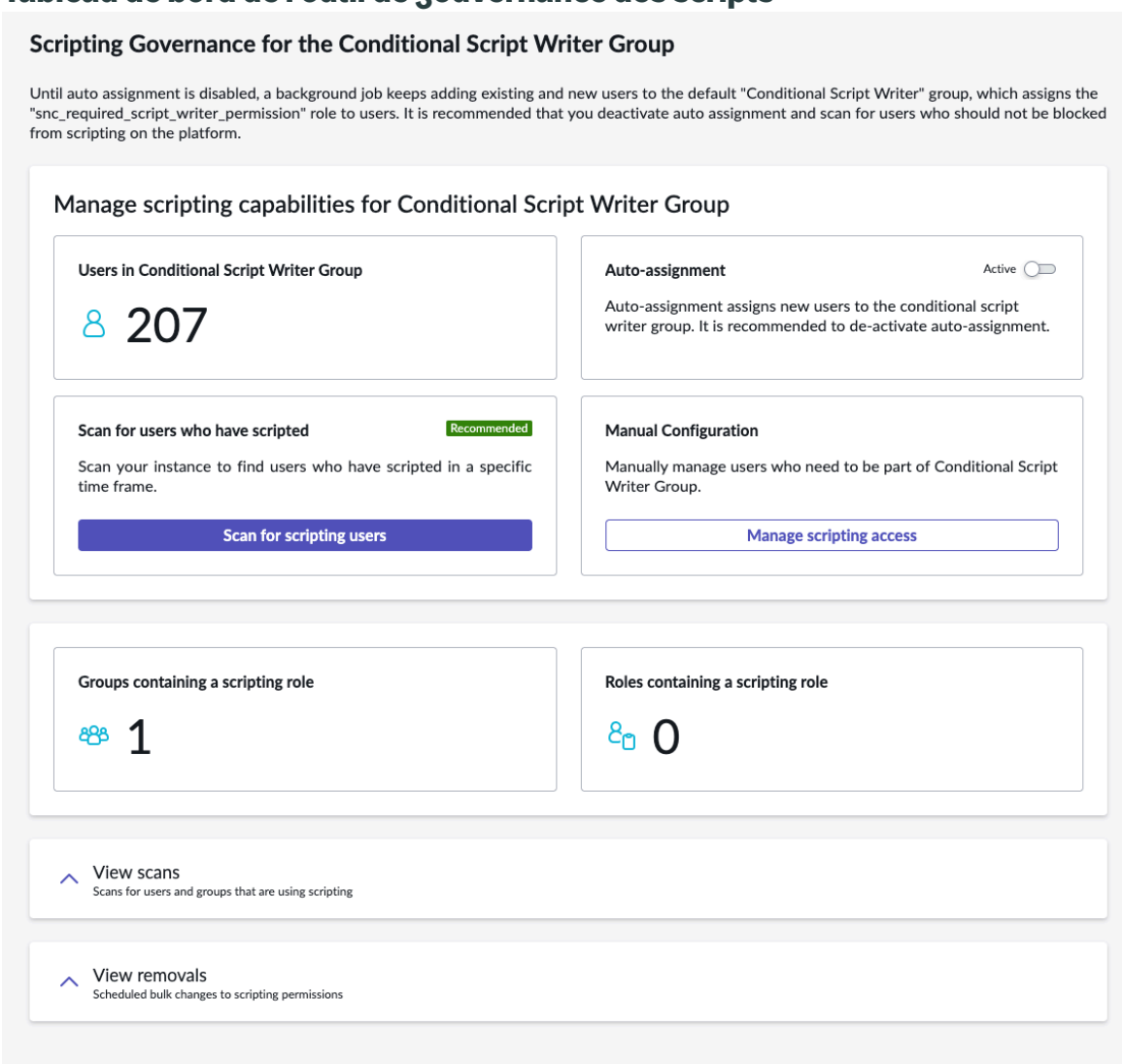
Outil de gouvernance de scripting

Gérez les autorisations utilisateur pour le scripting sur la plateforme à partir de l'outil de gouvernance de scripting.

L'outil de gouvernance des scripts vous aide à examiner les mesures de gouvernance des scripts d'utilisateur et à gérer le groupe d'auteurs de scripts conditionnels. Ce groupe accorde des autorisations de script à ses membres via le rôle snc_required_script_writer_permission. Les utilisateurs sont ajoutés au groupe par une affectation automatisée ou une configuration manuelle. Vous pouvez gérer ces deux paramètres à partir de **l'outil de gouvernance des scripts**.

Pour accéder à **l'outil de gouvernance des scripts,** accédez à **Tous** > **Sécurité de système** > **Outil de gouvernance de scripting**.

Tableau de bord de l'outil de gouvernance des scripts



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d’ensemble de l’outil de gouvernance des scripts

Utilisateurs du groupe d'auteurs de scripts conditionnels

Affiche le nombre d’auteurs dans le groupe Auteur de script conditionnel. Ces utilisateurs bénéficient de la snc_required_script_writer_permission jusqu’à ce qu’ils soient retirés du groupe.

Affectation automatique

L’affectation automatique affecte de nouveaux utilisateurs au groupe d’auteurs de scripts conditionnels ; sélectionnez le curseur pour activer ou désactiver l’affectation automatique

Analyse des utilisateurs qui ont scripté

Recherche les utilisateurs du groupe d’auteurs de scripts conditionnels qui ont écrit un script au cours de la période récente. Sélectionnez le bouton **Rechercher le scripting des utilisateurs** et remplissez le court formulaire pour planifier une analyse.

Configuration manuelle

Vous pouvez sélectionner manuellement les utilisateurs qui resteront dans le groupe Rédacteur de script conditionnel. Sélectionnez le bouton **Gérer l’accès aux scripts** et entrez les utilisateurs dans le champ de texte.

> **Remarque :**
> Les utilisateurs qui ne sont pas sélectionnés pour faire partie du groupe d’auteurs de scripts conditionnels seront planifiés pour être supprimés du groupe.

Groupes contenant un rôle de scripting

Affiche le nombre de groupes qui contiennent un rôle de script. Par défaut, le groupe d’auteurs de scripts conditionnels aura toujours un rôle de script.

Rôles impliquant un rôle de scripting

Affiche le nombre de rôles qui contiennent un rôle de scripting

Afficher les analyses

Table extensible contenant les utilisateurs et les groupes qui utilisent le scripting. Renseigné par le bouton **Rechercher le scripting des utilisateurs** .

Champs de la table d’analyse de script

Étiquette	Description
Numéro d'analyse	ID du numéro de la tâche d’analyse.
Statut	État de l’analyse
Terminé	État d’achèvement de l’analyse
Planifié	Heure d’exécution planifiée pour l’analyse
Créé par	Utilisateur ayant initié l’analyse
Action	Actions effectuées par l’analyse

Afficher les suppressions

Table extensible contenant les changements en bloc planifiés des autorisations de script. Elles sont renseignées soit par le widget **Analyser pour les utilisateurs en scripting** , soit par **configuration manuelle**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de table des suppressions

Étiquette	Description
Numéro de tâche de suppression	ID du numéro de la tâche de suppression.
Statut	État de la tâche de suppression
Terminé	État d'achèvement de la tâche de suppression
Planifié	Planifier l'heure d'exécution de la tâche de suppression
Créé par	Utilisateur à l'origine de la tâche de suppression

Contrôles d'accès à l'identité de machine

Définissez et appliquez des politiques de contrôle d'accès granulaires sur des ressources spécifiques pour les utilisateurs de l'intégration .

Les contrôles d'accès à l'identité de la machine permettent aux administrateurs de créer des politiques de contrôle d'accès granulaires pour les utilisateurs d'intégration. Cette couche de sécurité supplémentaire permet aux administrateurs de spécifier les ressources exactes (API REST, API SOAP et tables) auxquelles un utilisateur d'intégration peut accéder, garantissant ainsi une gouvernance des accès plus stricte.

Remarque :
Applicable aux utilisateurs marqués avec un accès au service Web uniquement.

Reportez-vous à la rubrique Créer un contrôle d'accès à l'identité de la machine pour savoir comment créer un contrôle d'accès à l'identité de la machine

Créer un contrôle d'accès à l'identité de la machine

Permettez aux administrateurs de définir et d'appliquer un contrôle granulaire pour les utilisateurs d'intégration en introduisant des profils d'accès utilisateur. Cette fonctionnalité fournit une couche supplémentaire de sécurité et de contrôle, permettant aux administrateurs de spécifier les ressources exactes (API REST ET API SOAP) auxquelles un utilisateur d'intégration peut accéder, garantissant ainsi une gouvernance plus stricte et minimisant les risques de sécurité.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Contrôles d'accès à l'identité de machine**.
2. Sélectionnez le bouton **Nouveau** .
3. Renseignez les champs du formulaire.

Champs de contrôle d'accès à l'identité de la machine

Champ	Description
Nom	Nom de l'enregistrement du contrôle d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Application contenant l’enregistrement.
Description	Description de l’enregistrement.
Actif	Détermine si la politique est active
Politique d’API REST	Sélectionnez la politique d’API REST cible. **Remarque :** Sélectionnez le et l’icône pour ajouter une politique.
Politique d’API SOAP	Sélectionnez la politique d’API SOAP cible. **Remarque :** Sélectionnez le et l’icône pour ajouter une politique.
Tables	Sélectionner les tables auxquelles cette politique s’applique
S’applique à la table enfant	Cocher cette option pour appliquer la politique aux tables enfants du champ **Tables**

4. Sélectionnez l’invite Insérer une ligne en dessous et ajoutez des utilisateurs auxquels appliquer le contrôle.
   Vous pouvez ajouter plusieurs utilisateurs au contrôle d’accès.

   Remarque :
   Vous ne pouvez sélectionner que des utilisateurs disposant d’un accès au service web.

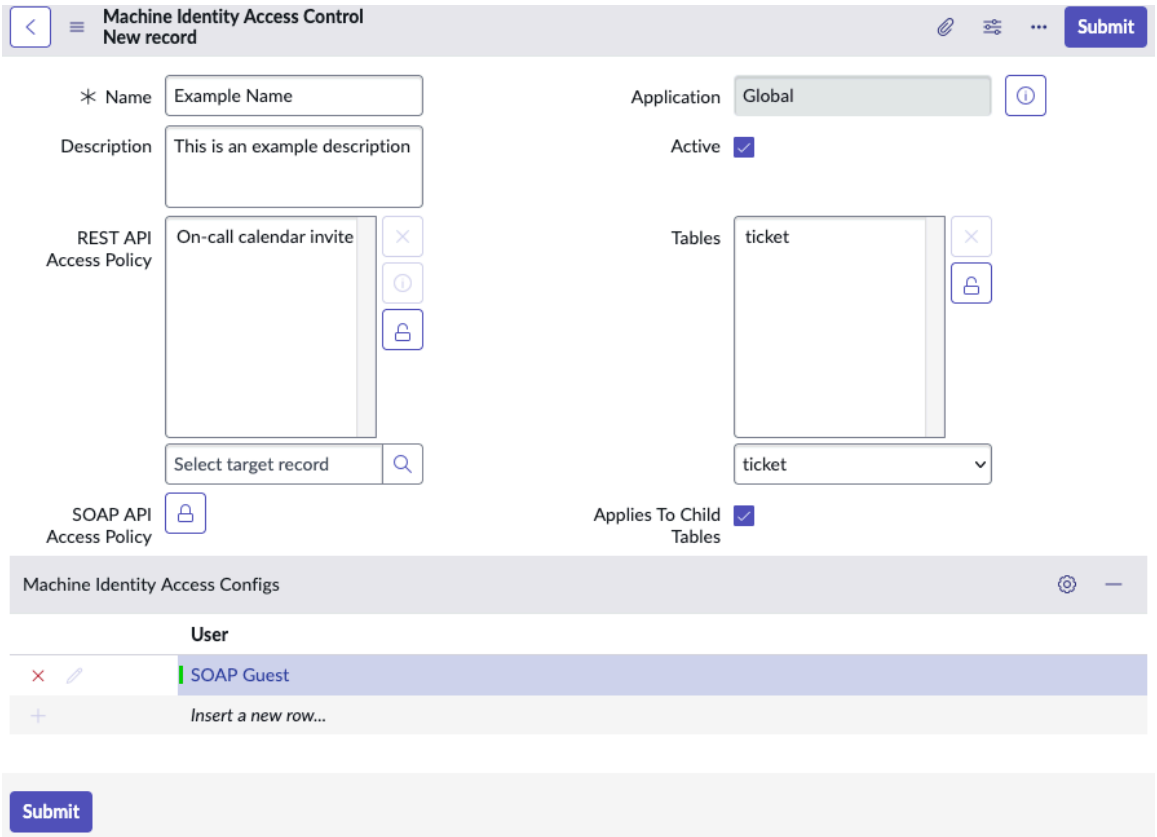
5. Sélectionnez **Soumettre**.

Résultats

Voici un exemple de formulaire de contrôle d’accès à l’identité de machine qui a été rempli :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un utilisateur disposant d'un contrôle d'accès à l'identité de la machine ne peut accéder à aucune autre API (REST ou SOAP) et ne pourra accéder qu'aux ressources explicitement indiquées dans le contrôle d'accès, même s'il dispose des rôles requis.

Filtration des données

Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

Important :

À partir de la version, la Yokohama filtration des données est en cours de préparation pour une dépréciation future. Elle sera masquée et ne sera plus activée sur les nouvelles instances. Envisagez d'utiliser des filtres de données de sécurité pour restreindre l'accès aux enregistrements en fonction du rôle ou des assertions liées à l'attribut de sécurité. Pour obtenir des détails, consultez Créer un filtre de données de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer la filtration des données



En savoir plus sur le filtrage des données.

Créer des règles de filtration des données



Créez vos propres règles de filtrage des données en fonction de vos besoins.

Déboguer les données



Découvrez comment déboguer vos résultats de filtration de données.

Traduction automatique

Explorer la filtration des données

Utilisez la filtration des données pour contrôler l’accès aux tables et aux enregistrements en fonction des attributs de sujet lors de l’exécution de requêtes de lecture.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La filtration des données est une forme distincte de contrôle d'accès conçue pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. La filtration des données refuse l'accès aux tables et aux enregistrements qui ne correspondent pas aux attributs de sujet définis par un administrateur. La filtration des données est conçue pour faciliter l'audit, la génération de rapports et le dépannage.

Il s'agit d'une fonctionnalité facultative que les administrateurs peuvent activer sur leur instance.

Fonctionnalités de filtration des données

Filtres de données

Utilisez des filtres de données pour accorder l'accès en fonction des informations contenues dans un enregistrement. Les filtres de données utilisent les données d'un champ de tables pour déterminer si un enregistrement est disponible pour vos utilisateurs.

Générateur de conditions basé sur l'attribut d'objet

Utilisez les attributs d'objet pour évaluer le rôle d'utilisateur, le groupe, les critères d'objet ou l'adresse réseau IP.

La filtration des données utilise un modèle basé sur un refus

La filtration des données utilise un modèle basé sur un refus pour contrôler l'accès aux enregistrements. Avec le filtrage des données, votre instance refuse l'accès aux enregistrements à moins qu'un enregistrement ne réponde aux critères définis par le filtrage des données.

Application de la filtration des données

Les règles de filtrage des données s'exécutent après la requête de base de données pour les opérations de lecture et sont évaluées avant les ACL. Un enregistrement refusé par une règle de filtrage de données ne sera pas traité et sera évalué par les règles ACL. L'application des règles de filtrage des données est cohérente avec celle des ACL de lecture.

Filtration des données et génération de rapports

La filtration des données et les ACL ne sont appliquées que lors de la création de rapports de vue de liste. Reporting n'applique pas de contrôle d'accès lors de la collecte de données agrégées. Dans ce cas, ni le filtrage des données ni les ACL ne sont vérifiés.

Pour les rapports agrégés, la filtration des données fonctionne conjointement avec les comportements existants *`Report_view access control list`* . Voir Contrôle d'accès Report_view pour plus de détails sur la configuration de ces contrôles de rapport.

Débogage de session

La filtration des données prend en charge le débogage de session. Utilisez le débogage de session pour voir quels enregistrements de filtration de données s'appliquent à une requête donnée. Les administrateurs peuvent utiliser ces informations pour résoudre les problèmes d'accès des utilisateurs aux enregistrements.

Composants de la filtration des données

La filtration des données fonctionne à l'aide des types d'enregistrement suivants :

Enregistrements de filtration des données

Créez un enregistrement de filtrage des données [sys_df_data_filtration] pour accorder l'accès à la table sur votre instance. L'enregistrement de filtrage des données contient les conditions de **filtre de données** et **d'attribut d'objet** décrites ci-dessus pour limiter le champ d'application de la règle et les utilisateurs affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

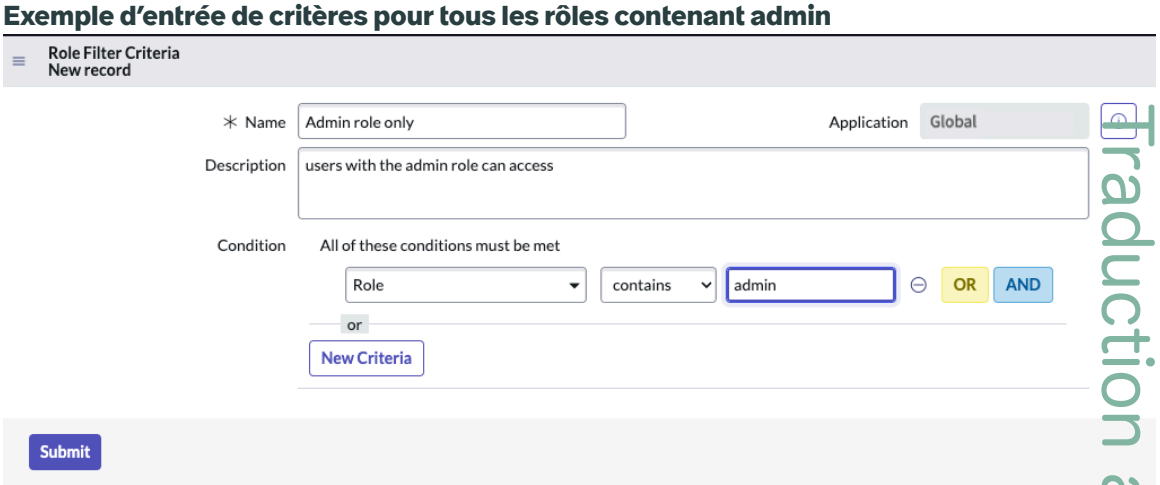
Enregistrements de critères de sujet

Les enregistrements Critères de sujet [sys_df_subject_criteria] représentent des attributs d'utilisateur spécifiques que vous pouvez utiliser pour déterminer s'il faut accorder l'accès avec une règle de filtrage de données. Ces attributs peuvent être les groupes, les rôles ou l'adresse IP d'un utilisateur. Pour créer un critère de sujet, vous devez créer l'enregistrement de critères de sujet, ainsi que les enregistrements d'entrée de critères et de conditions de critères. Pour obtenir des détails sur ce processus, consultez Créer des critères de sujet.

Après avoir créé des enregistrements de critères de sujet, vous pouvez les appliquer à une règle. Cette opération est effectuée dans l'onglet **Condition d'objet** de votre règle de filtrage des données.

Exemples d'enregistrements d'entrées de critères

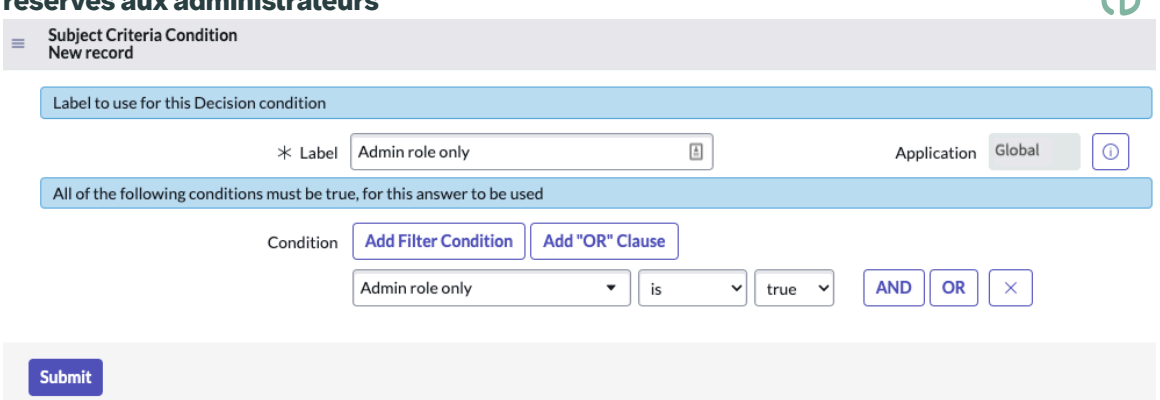
Exemple d'entrée de critères pour tous les rôles contenant admin



Les entrées de critères [sys_df_subject_filter_criteria_m2m] sont des enregistrements qui contiennent des critères à comparer avec l'utilisateur. Il peut s'agir d'une liste de groupes ou de rôles d'utilisateurs, d'une plage d'adresses IP ou d'un sous-réseau d'adresses IP. Ces enregistrements sont utilisés avec les enregistrements de conditions de critères de sujet pour les comparer aux groupes, rôles ou adresses IP d'un utilisateur afin de déterminer l'accès à une table ou à ses enregistrements.

Enregistrements des conditions des critères de sujet

Exemple de condition de critères utilisant l'entrée de critères réservés aux administrateurs



Utilisez les enregistrements de condition de critères de sujet [sys_df_subject_criteria_condition] pour définir comment comparer les attributs d'utilisateur avec les rôles, les groupes ou les adresses IP définis dans vos entrées de critères. Vous pouvez utiliser plusieurs entrées de critères dans une seule condition de critère de sujet pour affiner davantage l'accès à vos enregistrements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer la filtration des données

Découvrez comment activer la filtration des données sur votre instance.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**.
2. Utilisez le champ de recherche pour trouver le module d'extension Data Filtration (com.glide.data_filtration).
3. Cliquez sur **Installer**, puis cliquez sur **Activer** dans la boîte de dialogue Activer le module d'extension.

Créer des règles de filtration des données

Découvrez comment créer des règles de filtrage des données pour accorder l'accès de vos utilisateurs aux enregistrements sont des tables.

Avant de commencer
Rôle requis : security_admin

Remarque :
Pour créer ou modifier des règles de filtrage de données, vous devez vous élever au rôle privilégié. Pour plus de détails sur ce processus, voir Élever à un rôle privilégié.

Procédure

1. Accédez à la **Tous** > **Filtration des données** > **Enregistrements de filtration des données**.
2. Cliquez sur **Nouveau** dans la liste **Filtration des données** .
   Un nouveau formulaire de filtration des données s'affiche.
3. Dans le formulaire, renseignez les champs selon vos besoins.

Formulaire de filtration des données

Champ	Description
Table	Table à laquelle cette règle de filtrage des données s'applique. **Remarque :** Les utilisateurs n'ayant pas accès à la maintenance ne peuvent pas créer de filtrage de données sur certaines tables. Pour contourner ce problème, supprimez l'attribut tableChoicesScript=DataFiltrationTableList, mais assurez-vous qu'aucun filtre ne sera créé sur les tables sys_df_xxx ou les tables du sys_df_table_exclusion.
Actif	Définit la règle de filtration des données comme active. **Remarque :** Conservez les règles de filtration des données inactives jusqu'à ce que vous soyez prêt à effectuer le test pour éviter de bloquer involontairement l'accès des utilisateurs aux enregistrements.
Description	Description de la règle de filtrage des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
En cascade	Sélectionnez cette option pour définir la règle de filtration des données à appliquer aux tables étendues. Par exemple, vous sélectionnez la table Tâche [task] et activez la mise en cascade. Dans ce cas, la règle de filtrage des données s'applique également à toutes les tables étendues à partir de la tâche, telles que Incident[incident] et Demande de changement[change_request]. Pour en savoir plus sur l'extension de table, reportez-vous à la rubrique Table extension and classes **Remarque :** Ce champ est activé par défaut.

4. **Facultatif :** Pour affiner le champ d'application de la règle, renseignez les champs **Conditions** selon vos besoins.

Champ	Description
Condition de sujet	Toutes les conditions doivent être remplies pour y accéder.
Condition d'attribut de sécurité	Toutes les conditions doivent être remplies pour y accéder. **Local** L'attribut n'est défini que dans le cadre de la règle de filtrage des données. **existant** L'attribut est défini par référence à un **attribut de sécurité** déjà existant
Condition de données	Définit les conditions pour que les données soient soumises à la règle. **Remarque :** Une condition de données vide s'appliquera à tous les enregistrements de la table sélectionnée.

5. Sélectionnez **Enregistrer** dans le menu du formulaire.
Une fois que vous avez enregistré votre règle de filtrage des données, cette règle s'applique automatiquement à tous les enregistrements de la table sélectionnée, sauf indication contraire dans la condition de données.

Ajouter un filtre de données pour votre règle de filtration de données

Vous pouvez éventuellement utiliser un filtre de données pour affiner le champ d'application de votre règle de filtrage des données afin qu'elle ne s'applique qu'à des enregistrements spécifiques d'une table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

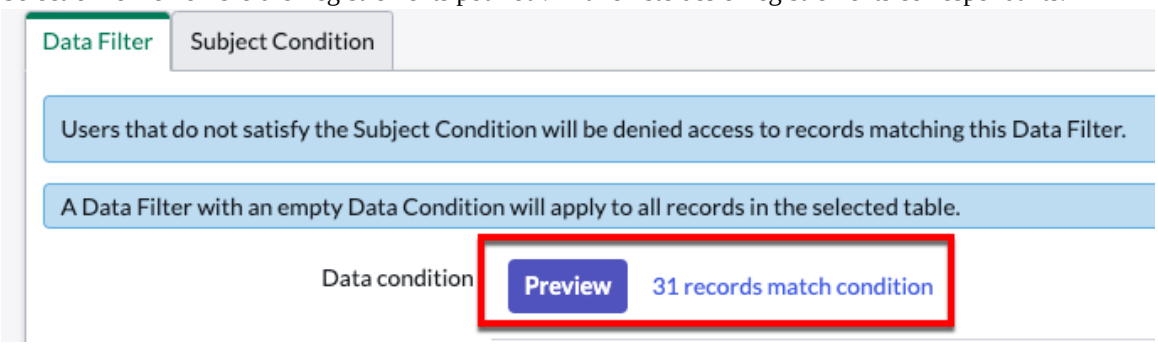
Rôle requis : admin

Procédure

1. Dans votre enregistrement de filtration, ouvrez l'onglet **Filtre de données** .
2. Utilisez le générateur de conditions pour filtrer les enregistrements de table leurs valeurs de champ.
   Le filtre de données utilise le même générateur de conditions que celui utilisé dans d'autres parties de la plateforme. Pour plus d'informations sur l'utilisation de cette interface, voir Créateur de conditions .

> **Important :**
> L'onglet **Filtre de données** apparaît vide jusqu'à ce que vous sélectionniez une table dans le champ **Table** .

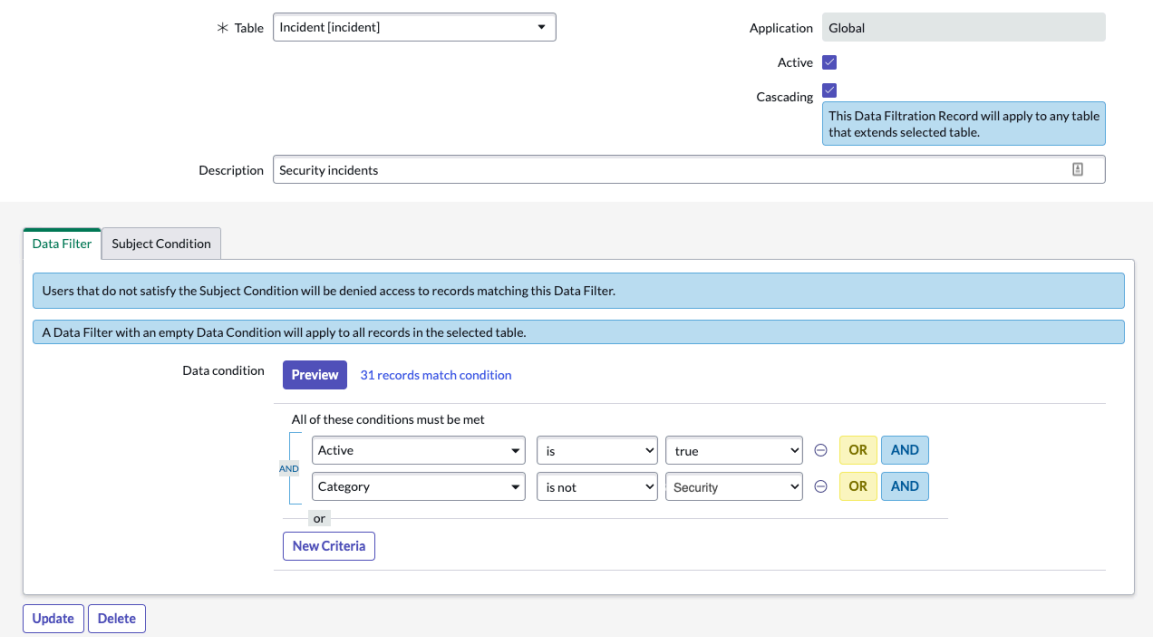
3. Utilisez le bouton **Aperçu** pour voir le nombre d'enregistrements correspondant à votre filtre de données.
4. Sélectionnez le nombre d'enregistrements pour ouvrir une liste des enregistrements correspondants.



5. Sélectionnez **Enregistrer**.

Example:

Cet exemple montre une règle de filtrage des données pour la table Incident [incident]. Le filtre de données est défini pour sélectionner tous les enregistrements actifs qui ne sont pas dans la catégorie **Sécurité** . Avec cette règle active, les utilisateurs peuvent voir ces enregistrements. Voir la section ci-dessous pour une utilisation plus approfondie des critères en dehors du contenu de l'enregistrement.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

L'opération not dans vos conditions peut renvoyer des résultats inattendus, selon le type de base de données que votre instance utilise. Par exemple, prenez la condition suivante :

Pour cette condition, le résultat attendu serait que l'ensemble de résultats serait tous les enregistrements où la société n'est pas ServiceNow et tous les enregistrements qui n'ont pas de valeur dans le champ **Société** . Les instances utilisant des bases de données autres que MySQL et Maria ne renvoient pas d'enregistrements de valeurs avec un champ **d'entreprise** vide. Lorsque vous utilisez des requêtes **non** pour ces instances, incluez des conditions pour vous assurer que les valeurs vides sont renvoyées.

Ajouter des attributs d'objet à votre règle de filtrage des données

Vous pouvez éventuellement utiliser des attributs d'objet pour affiner le champ d'application de votre règle de filtrage de données en fonction d'attributs tels que l'adresse réseau IP, les groupes et rôles d'utilisateurs ou les critères d'objet.

Avant de commencer

Rôle requis : admin

Procédure

1. Dans votre enregistrement de filtration, ouvrez l'onglet **Critères de sujet** .
2. Utilisez le générateur de conditions pour filtrer les enregistrements de table en fonction d'un ou plusieurs des critères suivants.

Options de critères de sujet

Option	Description
Critères réseau	Permet l'accès aux enregistrements en fonction de la plage d'adresses IP du réseau ou du sous-réseau IP.
Critères de sujet	Permet l'accès à des enregistrements en fonction de critères de sujet. Sélectionnez un enregistrement de critères de sujet pour appliquer ses conditions à votre règle de filtrage de données. Pour plus d'informations sur la création d'enregistrements de critères de sujet, reportez-vous à la section Créer des critères de sujet.
Groupe de sujets	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe dans la table **Groupes**[sys_user_group].
Rôle du sujet	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe dans la table **Rôles** [sys_user_role].

Important :

Les conditions de critères de sujet ne prennent en charge que l'opérateur **is** .

3. Après avoir ajouté vos critères de sujet, cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des critères de sujet

Créez des enregistrements de critères de sujet à utiliser dans les règles de filtrage des données.

Avant de commencer
Rôle requis : security_admin

Important :
Pour créer ou modifier des règles de filtrage de données, vous devez vous élever à un rôle privilégié. Pour plus de détails sur ce processus, voir Élever à un rôle privilégié.

Procédure

1. Accédez à la **Tous** > **Filtration des données** > **Critères de sujet**.
2. Dans la liste **Critères de sujet** , cliquez sur le bouton **Nouveau** .
   Un nouveau formulaire de critères de sujet s'affiche.
3. Dans le formulaire, renseignez les champs selon vos besoins.

Champs des critères de sujet

Champ	Description
Nom	Nom des critères de sujet.
Application	Application incluse dans le champ d'application pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuel.
Description	Description des critères de sujet.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer** dans le menu contextuel.
   Après l'enregistrement, les champs **Entrées de critères** et **Conditions de critères** s'affichent.

Créer une entrée de critères de sujet

Créez une entrée de critères de sujet pour définir les critères sur lesquels vos règles de filtrage de données filtrent.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Sur l'enregistrement de vos critères de sujet, ouvrez l'onglet **Entrées de critères** .
2. Dans la liste **Entrées de critères** , cliquez sur **Nouveau**.
3. Sélectionnez l'entrée de politique pour les critères que vous souhaitez créer.

Entrées de la politique

Entrée de politique	Description
Critère de filtre d'adresses IP	Créer une entrée de politique basée sur l'adresse IP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Entrée de politique	Description
Critère de filtre de rôle	Créer une entrée de politique basée sur le rôle d'utilisation
Critères de filtre de groupe	Créer une entrée de politique basée sur le groupe d'utilisateurs

Un **formulaire Critère de filtre IP**, **Critère de filtre de rôle** ou **Critère de filtre de groupe** s'affiche, en fonction de votre sélection à cette étape.

4. Dans le formulaire Critères de filtre, renseignez les champs selon vos besoins.

Champs de critères de filtre

Champ	Description
Nom	Nom des critères de filtre
Application	Application incluse dans le champ d'application pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuel.
Description	Description du critère de filtre

5. Sous les champs de formulaire se trouvent des onglets utilisés pour définir les adresses IP, les groupes ou les rôles pour les entrées de critères de filtre.

Filtrer les champs de critères pour des types d'entrées spécifiques

Type d'entrée de politique	Description	Création
Critère de filtre d'adresses IP	Critères de filtre IP de l'utilisateur pour créer une plage ou un sous-réseau d'adresses IP. Vos critères de sujet peuvent ensuite être comparés à l'adresse IP de l'utilisateur par rapport à cette plage ou sous-réseau.	Utilisez la **plage IP** ou **sous-réseau (CIDR)** pour définir des adresses IP pour votre entrée. **Plage IP** Dans la liste **Plages IP** , double-cliquez sur **Insérer une nouvelle ligne** et entrez une adresse IP de départ dans l'adresse **IP de départ**. Ensuite, appuyez sur la touche de tabulation et entrez une adresse IP de fin dans le champ **Adresse IP de fin** . Enfin, appuyez sur Entrée pour enregistrer l'entrée de liste. **Sous-réseau (CIDR)** Dans la liste **Sous-réseaux** , double-cliquez sur **Insérer une nouvelle ligne** et entrez une adresse IP de réseau dans le champ **Adresse IP** réseau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d'entrée de politique	Description	Création
		Ensuite, appuyez sur la touche de tabulation et entrez un masque réseau dans le champ **Masque réseau** . Enfin, appuyez sur Entrée pour enregistrer l'entrée de liste. **Remarque :** Les travaux planifiés déclenchés par un planificateur ne sont pas destinés à filtrer les données à l'aide d'un critère de réseau, car ils n'ont pas le contexte de l'adresse IP du client demandeur. Un type de filtration plus approprié peut être la condition de sujet Rôle/Groupe.
Critère de filtre de rôle	Utilisez les critères de filtre de rôles pour créer une sélection de rôles. Vos critères de sujet peuvent ensuite être comparés aux rôles affectés à l'utilisateur par rapport à cette sélection.	Utilisez le générateur de conditions dans le **champ Condition** pour sélectionner des rôles pour votre entrée.
Critères de filtre de groupe	Utilisez des critères de filtre de groupe pour créer une sélection de groupes d'utilisateurs. Vos critères de sujet peuvent ensuite être comparés avec les groupes affectés de l'utilisateur par rapport à cette sélection.	Dans le tableau **Groupes pour critères** , double-cliquez sur **Insérer une nouvelle ligne** et sélectionnez un groupe d'utilisateurs. Appuyez sur Entrée ou cliquez sur l'icône de coche verte pour enregistrer le groupe. Cliquez sur le texte **Insérer une nouvelle ligne** sous la première entrée pour créer des entrées supplémentaires.

6. Après avoir défini votre entrée, cliquez sur **Soumettre**.

Remarque :
En plus de créer des entrées de critères pour vos critères de sujet, vous pouvez également ajouter des entrées existantes. Cliquez sur **Modifier** dans l'onglet **Entrées de critères** , puis sélectionnez une entrée existante.

Créer une condition de critères de sujet

Créez une condition pour comparer les informations d'un utilisateur à l'entrée de critères de sujet existante.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les conditions de critères comparent les attributs de l'utilisateur aux entrées de critères existants pour déterminer s'il faut autoriser l'accès aux enregistrements. Pour créer une condition de critère, vous devez avoir créé des critères de sujet. Pour plus de détails sur ce processus, Créer une entrée de critères de sujet reportez-vous à la section .

Procédure

1. Sur votre enregistrement de critères de sujet, ouvrez l'onglet **Conditions de critères** .
2. Dans la liste **Conditions de critères** , cliquez sur **Nouveau**.
3. Renseignez les champs selon vos besoins dans le formulaire **Condition de critères de sujet** .

Formulaire de condition de critères de sujet

Champ	Description
Étiquette	Une étiquette descriptive pour votre condition
Application	Application incluse dans le champ d'application pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuel.

4. Créez une condition pour votre condition de critères de sujet à l'aide du générateur de conditions en sélectionnant l'une des options de condition suivantes.
   Ces options de condition incluent toutes les entrées de critères de sujet que vous avez créées.
5. **Facultatif :** Créez d'autres conditions en cliquant sur les boutons **Ajouter une condition de filtre** ou **Ajouter une clause « OU ».**

   Remarque :
   À moins que vos conditions ne soient séparées par une clause **ou** , toutes les conditions doivent être évaluées comme vraies pour que la condition des critères de sujet soit évaluée comme vraie.

6. Cliquez sur **Soumettre** pour enregistrer la condition de critères de sujet.

Que faire ensuite

Utilisez des critères de sujet dans vos règles de filtrage des données pour limiter l'accès aux tables et aux enregistrements. Pour plus d'informations sur l'utilisation des critères de sujet dans les règles de filtrage des données, reportez-vous à la section Créer des critères de sujet.

Débogage de la filtration des données

Utilisez le journal de session pour voir comment la filtration des données affecte vos enregistrements et déboguer les problèmes d'accès des utilisateurs.

Avant de commencer

Rôle requis : admin

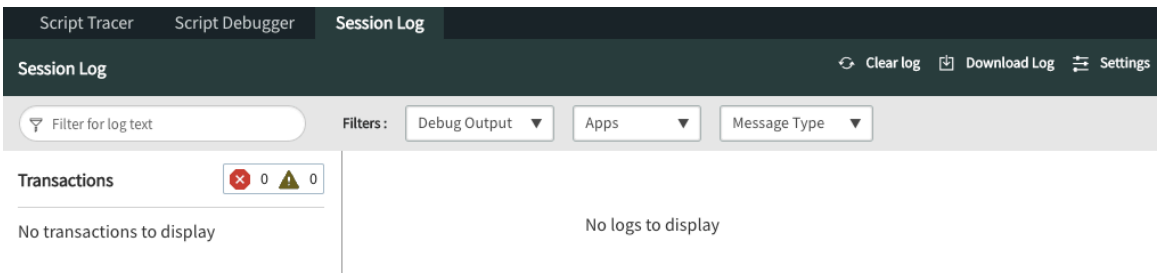
Les informations de sortie s'affichent dans les journaux de session lorsque les utilisateurs accèdent aux enregistrements. Vous pouvez utiliser ces informations de journalisation avec l'emprunt d'identité pour savoir pourquoi les utilisateurs voient ou ne voient pas les enregistrements. Vous pouvez ensuite utiliser ces informations pour ajuster vos règles de filtrage des données et vous assurer que les utilisateurs ne voient que ce que vous voulez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Débogage** > **Déboguer toute la sécurité**.
   Le **débogueur de script** s'ouvre dans un nouvel onglet ou une nouvelle fenêtre de navigateur.



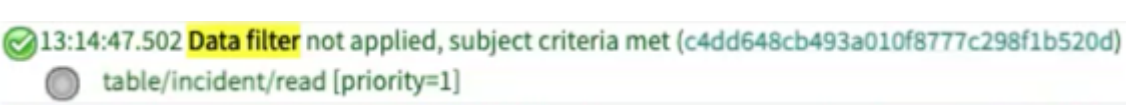
2. Dans la fenêtre **Débogueur de script** , sélectionnez l'onglet **Journal de session** .
3. Dans un autre onglet ou une autre fenêtre de navigateur, empruntez l'identité d'un utilisateur pour résoudre les problèmes d'accès de cet utilisateur.

> **Remarque :**
> L'emprunt d'identité permet à un administrateur de voir une instance avec les paramètres et l'accès d'un autre utilisateur. Pour plus de détails sur l'emprunt d'identité, consultez Emprunter l'identité d'un utilisateur .

4. Lorsque vous empruntez l'identité d'un utilisateur, accédez à une liste ou à un enregistrement où vous constatez un comportement inattendu.
   Ce comportement peut être un enregistrement que l'utilisateur voit, mais ne devrait pas voir, ou une liste d'enregistrements qui n'apparaissent pas comme prévu pour un utilisateur.
   Après avoir accédé aux enregistrements avec l'utilisateur dont l'identité a été empruntée, vous devez commencer à voir la sortie dans le débogueur de session.
5. Recherchez les informations de filtration des données dans le débogueur de session.



Cet exemple montre deux messages de journal dans lesquels un filtre de données a refusé l'accès à des enregistrements. Les entrées de journal apparaissent sous forme de texte rouge et incluent la raison pour laquelle le filtre de données a refusé l'accès, ainsi que la sys_id du filtre de données. Vous pouvez cliquer sur cette sys_id pour ouvrir l'enregistrement de filtrage des données.



Cet exemple montre un message de journal dans lequel un filtre de données autorise l'accès à un enregistrement. Ces entrées de journal apparaissent sous forme de texte vert. Comme pour le premier message, vous pouvez cliquer sur cette sys_id pour ouvrir l'enregistrement de filtrage des données.

6. Utilisez ces informations pour apporter des ajustements à vos règles de filtrage des données.
   Répétez ces étapes pour affiner vos règles et donner aux utilisateurs l'accès dont ils ont besoin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[store-future: BEGIN review]

Bonnes pratiques en matière de filtre de données

Document de souche pour le test

Document de souche pour le test

[End]

Filtres de données de sécurité

Les filtres de données de sécurité restreignent l'accès aux enregistrements en fonction du rôle ou des assertions liées à l'attribut de sécurité.

Exploration des filtres de données de sécurité

Les filtres de données de sécurité permettent de restreindre l'accès aux enregistrements en fonction du rôle d'un utilisateur ou d'autres affirmations liées à un attribut de sécurité. Les filtres de données de sécurité garantissent que seuls les utilisateurs autorisés peuvent afficher les enregistrements, quelle que soit la manière dont ils accèdent aux données.

Les filtres de données de sécurité sont appliqués avant l'exécution d'une requête afin que les données restreintes ne quittent jamais la base de données. En revanche , les ACL conditionnelles filtrent les données après l'exécution d'une requête, ce qui peut entraîner une fuite de données.

Remarque :
Associez des filtres de données de sécurité à ACL refuser, sauf pour garantir une sécurité cohérente

Fonctionnalités des filtres de données de sécurité

Les principales caractéristiques des filtres de données de sécurité sont les suivantes :

- Les filtres de données de sécurité sont appliqués dans la requête.
- Conditions de filtre des données de sécurité ET à la requête sur la table cible et entre elles.
- Les filtres de données de sécurité ne sont pas vérifiés par `canRead`. Voir Quand utiliser les filtres de données de sécurité pour plus de détails
- Les règles de définition du champ d'application des filtres de données sont basées sur le champ d'application de la table, les filtres de données ne suivent pas les règles de champ d'application ScopeMaster ou sys_scope

Application et application du filtre de données de sécurité

En général, les filtres de données de sécurité sont appliqués après les ACL absolues (également appelées ACL au niveau de la table) et après les ACL de ligne. Les filtres de données de sécurité sont appliqués par défaut et ont un impact sur le comportement du système s'ils ne sont pas utilisés avec précaution. Consultez la liste Filtres de sécurité par défaut des filtres de données de sécurité par défaut.

Les filtres de données de sécurité ne sont appliqués qu'aux requêtes GlideRecordSecure, GlideRecordSandbox et GlideAggregateSandbox par défaut. Il existe deux nouvelles API GlideRecord `enableSecurityFeature` et `disableSecurityFeature` qui peuvent être utilisées dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les scripts Java et côté serveur pour activer ou désactiver les filtres de données pour une requête spécifique.

Important :
Vous devez activer explicitement les filtres de données pour les requêtes destinées aux utilisateurs qui n'utilisent pas GlideRecordSecure.

Quand utiliser les filtres de données de sécurité

Les filtres de données de sécurité sont les mieux adaptés pour :

- Empêcher les données sensibles de quitter la base de données
- Supprimer le message « lignes cachées par la sécurité »
- Empêcher les fuites de données sensibles par le biais de rapports

Quand ne pas utiliser les filtres de données de sécurité

Les filtres de données de sécurité ne doivent pas être utilisés :

- En tant que contrôle de visibilité
- En remplacement des ACL
- Avec un grand nombre de conditions de filtre
- Sur les colonnes non indexées

Comportement du filtre de données de sécurité

Plusieurs filtres de données de sécurité se combinent pour l'évaluation, comme un `ET` combine des opérandes. À titre d'exemple, trois filtres de données de sécurité sont donnés :

- Filtre 1 : « actif = vrai »
- Filtre 2 : `priority=1`
- Filtre 3 : `état=ouvert`

Et une première question :

```
SELECT * FROM task WHERE state != closed AND active = true AND
    priority = 1
```

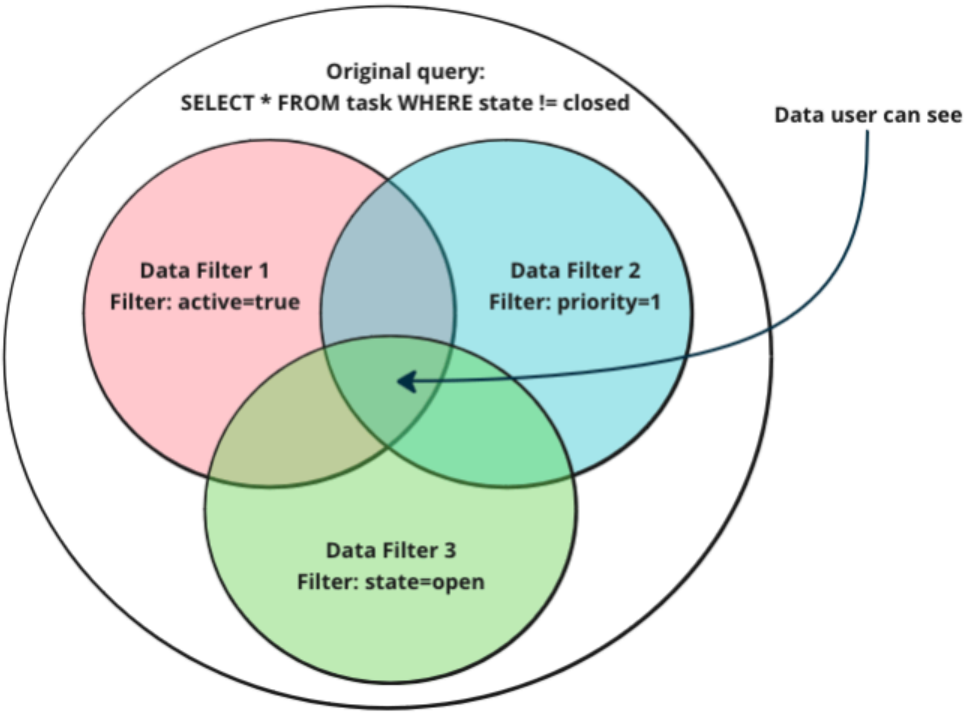
La dernière requête est la suivante :

```
SELECT * FROM task WHERE state != closed
    AND active = true AND priority = 1 AND state = open
```

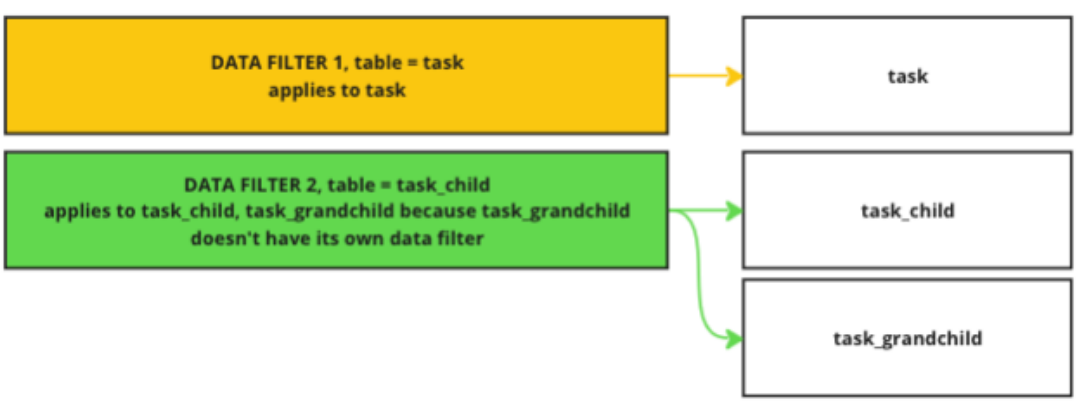
Voir le diagramme ci-dessous pour une représentation visuelle de cet exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une différence importante dans la façon dont les filtres de données de sécurité et les ACL sont appliqués est que les filtres de données d'une table enfant ne s'appliquent pas à la table parente lorsque les données sont interrogées à partir de la table parente. Ajoutez un filtre de données sur les tables enfant et parent pour restreindre l'accès aux enregistrements de la table parente. Le diagramme ci-dessous met en évidence la hiérarchie :



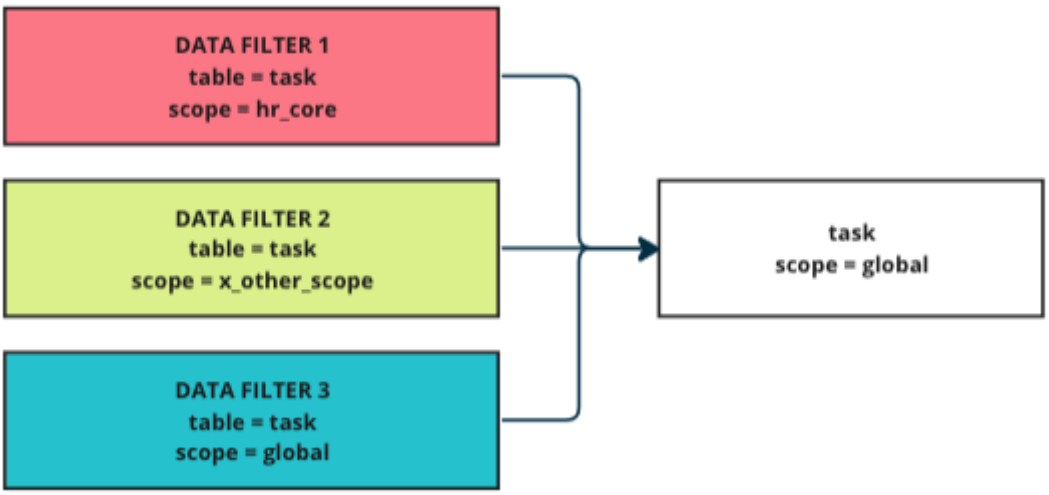
Remarque :
Une solution courante consiste à ajouter un filtre de données sur le parent qui masque complètement les enregistrements enfants dans la table parente.

Les filtres de données sont appliqués avec des règles de définition du champ d'application similaires aux ACL, mais avec quelques

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

différences clés car les filtres de données s'appliquent avant la



requête.

Créer un filtre de données de sécurité

Découvrez comment créer des règles de filtre de données de sécurité pour accorder l'accès de vos utilisateurs aux enregistrements sont des tables.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Filtres de données de sécurité**.
2. Cliquez sur **Nouveau** dans la liste **Filtres de données de sécurité** .
3. Dans le formulaire, renseignez les champs selon vos besoins.

Formulaire de filtration des données

Champ	Description
Nom de la table	La table à laquelle le filtre de données de sécurité s'applique.
Description	Description de la règle de filtrage des données de sécurité.
Actif	Définit la règle de filtrage des données de sécurité comme active. **Remarque :** Conservez les règles de filtrage des données de sécurité inactives jusqu'à ce que vous soyez prêt à effectuer le test afin d'éviter d'exclure involontairement les utilisateurs des enregistrements.
Afficher dans l'interface utilisateur	Détermine si une notification sera affichée dans l'interface utilisateur si le filtre de données de sécurité s'applique à une requête
Application	Le périmètre de l'application du filtre de données de sécurité.
Mode	Le mode du filtre de données.
Filtre	Condition de filtre qui détermine les enregistrements auxquels le filtre de données s'applique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Attributs de sécurité	Les attributs de sécurité qui contrôlent si le filtre de données s'appliquera ou non

4. Sélectionnez **Enregistrer** dans le menu du formulaire.

Résultats
Une fois que vous avez enregistré votre règle de filtrage des données de sécurité, cette règle s'applique automatiquement à tous les enregistrements de la table sélectionnée, sauf indication contraire dans la condition de données.

Filtres de sécurité par défaut

En général, les filtres de données sont appliqués après les ACL absolues (parfois appelées ACL au niveau de la table) et après les ACL au niveau de la ligne. Elles sont appliquées par défaut et peuvent avoir un impact sur le comportement du système si elles ne sont pas utilisées avec précaution.

Filtres de données de sécurité appliqués par défaut

Les filtres de données de sécurité sont appliqués par défaut aux emplacements suivants :

Catégorie	Application
Liste et formulaires	• UI16 • Espaces de travail • Catalogue de services • Portail de services • Mobile
Rapports et tableaux de bord	• Rapports • Visualisations des données • Tableaux de bord de l'interface utilisateur principale • Tableaux de bord de l'expérience Platform Analytics
Exportation de données	• Exporter XML • CSV • Excel • JSON • PDF
Moteur de flux	Étapes de la recherche d'enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Application
Rechercher	• Recherche IA • Recherche de texte
GlideRecord	• GlideRecordSecure • Bac à sable GlideRecordBox • Bac à sable GlideAggregate
API REST et GraphQL	• REST table API • API de statistiques REST • Équivalent de la table et de l'API de statistiques GraphQL

Rôles de sécurité

Les rôles de sécurité offrent une sécurité supplémentaire. Chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse distinguer les utilisateurs internes des utilisateurs externes.

Explorer les rôles explicites



Découvrez les principales fonctionnalités et la valeur commerciale des rôles explicites.

Explorer le privilège élevé



Découvrez comment le rôle de privilège élevé active les privilèges basés sur la session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explicit Roles

Vous pouvez donner l'accès à votre instance à la fois aux utilisateurs internes et aux utilisateurs externes. Cependant, vous ne souhaitez peut-être pas donner le même niveau d'accès à ces deux types d'utilisateurs. Pour fournir une sécurité accrue, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

Pour la version Paris, aucun utilisateur ne peut avoir les deux rôles explicites (snc_internal et snc_external). Les groupes et le rôle de confinement ne peuvent pas inclure les deux rôles, car cela aurait pour conséquence qu'un membre du groupe ou un utilisateur qui est affecté à un tel groupe ou un tel rôle recevrait automatiquement les deux rôles. ServiceNow AI Platform abandonne toute opération qui créerait un tel scénario.

Remarque :
Vous ne pouvez pas ajouter d'autres rôles en tant que rôles contenus aux rôles «*snc_external*» ou «*snc_internal*».

Les utilisateurs externes doivent au minimum obtenir le rôle snc_external. Le rôle snc_external indique que l'utilisateur est externe à votre organisation. Il ne doit pas avoir accès aux ressources à moins d'y être explicitement autorisé par les ACL pour le rôle snc_external ou pour des rôles supplémentaires qui héritent du rôle snc_external. Par défaut, les utilisateurs dotés du rôle snc_external ne peuvent pas accéder aux éléments suivants :

- Tables sans le rôle qui hérite du rôle snc_external ou du rôle public.
- Les ressources de type autre qu'un enregistrement, telles que les processeurs et les pages de l'interface utilisateur, n'accordant pas l'accès au rôle snc_external ou à un rôle qui hérite du rôle snc_external.
- Tableaux de bord Platform Analytics.

Ne marquez pas le rôle snc_internal comme élevé. Sinon, les utilisateurs internes ne pourront pas accéder à l'instance.

Module d'extension Explicit Roles

Lorsque le module d'extension Explicit Roles est activé :

- Tous les Les utilisateurs doivent disposer du rôle snc_internal pour accéder aux ressources internes ou du rôle snc_external pour accéder aux ressources externes. Les utilisateurs sans rôle explicite ne peuvent accéder qu'aux ressources publiques.
- Tous les utilisateurs existants se voient affecter automatiquement le rôle snc_internal. Ce rôle ne modifie pas les niveaux d'accès existants ni le comportement du système. Au lieu de cela, il fournit une catégorie pour différencier les utilisateurs internes des utilisateurs externes. Tous les utilisateurs internes maintiennent le même niveau d'accès qu'avant l'activation du module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :
Pour éviter de modifier les fonctionnalités existantes pour les utilisateurs, l'activation du module d'extension Explicit Roles affecte le rôle d'utilisateur snc_internal à tous les utilisateurs existants dans l'instance. Cela inclut tous les utilisateurs externes ajoutés avant que le module d'extension Explicit Roles ait été activé. Après avoir activé le module d'extension Explicit Roles, effectuez les actions suivantes pour tous les utilisateurs externes ajoutés avant l'activation du module d'extension Explicit Roles :

- Supprimez le rôle snc_internal.
- Ajoutez le rôle snc_external.

Cela garantit que les utilisateurs externes ajoutés avant l'activation du module d'extension Explicit Roles n'ont pas accès aux ressources internes qui ne doivent être disponibles que pour les utilisateurs internes.

- Les utilisateurs nouvellement créés se voient affecter automatiquement le rôle snc_internal lorsqu'ils tentent pour la première fois de se connecter à l'instance, à moins que le rôle snc_external ne leur ait été explicitement affecté. Vous pouvez ajouter le rôle snc_external à un nouvel utilisateur avant qu'il ne se connecte pour la première fois à l'instance pour lui fournir des droits d'utilisateur externe.

  Important :

  Activez ce module d'extension pendant une fenêtre de maintenance ou lorsque peu d'utilisateurs sont connectés. Les utilisateurs actuellement connectés lorsque le module d'extension est activé ne se verront pas attribuer dynamiquement le rôle snc_internal. Les utilisateurs doivent plutôt se déconnecter et se reconnecter pour se voir affecter le rôle snc_internal. Une fois le module d'extension activé, vous pouvez ajouter ou supprimer les rôles snc_internal et snc_external à tout moment pour changer les droits des utilisateurs.

  Une fois que le module d'extension est activé, chaque fois qu'un utilisateur se connecte, il reçoit le rôle snc_internal si le compte n'a pas déjà ce rôle ou celui de snc_external. Cela inclut les utilisateurs connectés via l'emprunt d'identité.

- Tous les ACL existants qui n'ont pas de rôle requis se voient affecter automatiquement le rôle snc_internal. Étant donné que le rôle snc_internal est affecté aux ACL comme aux utilisateurs existants, les niveaux d'accès existants ne changent pas.
- Les ACL nouvellement créés qui n'ont pas de rôle requis se voient affecter automatiquement le rôle snc_internal. Cette affectation de rôle ne s'applique pas à un ACL nouvellement créé avec un rôle affecté.
- Pour tous les enregistrements de processeur [sys_processor] existants ou les enregistrements de processeur [sys_processor] nouvellement créés avec **Type = script**, le rôle snc_internal est automatiquement ajouté au champ **Rôles** si celui-ci est vide.
- Pour restreindre l'accès aux pages de l'interface utilisateur aux utilisateurs internes, le module d'extension affecte automatiquement le rôle snc_internal à l'ACL ***** avec un **type** de **ui_page**.
- Pour restreindre l'accès aux processeurs aux utilisateurs internes, le module d'extension affecte automatiquement le rôle snc_internal à l'ACL ***** avec un **type** de **processeur**.
- Les utilisateurs externes doivent au minimum obtenir le rôle snc_external pour accéder à l'instance. Ce rôle doit être accordé manuellement aux utilisateurs externes. L'accès aux enregistrements est accordé par l'intermédiaire des ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ne déplacez pas les ensembles de mises à jour système entre les instances avec et sans le module d'extension Explicit Roles activé. Pour plus d'informations, consultez Ensembles de mises à jour système .

Remarque :
Ce module d'extension nécessite également le module d'extension Contextual Security Manager.

Comportement glide.security.explicit_roles.do_not_fix

À partir de la Xanadu version , le glide.security.explicit_roles.do_not_fix a été ajusté avec des modifications apportées à snc_internal. Le rôle snc_internal est maintenant le même en mémoire et en sys_user_has_role. Le nouveau comportement de glide.security.explicit_roles.do_not_fix est le suivant :

Nouveau comportement glide.security.explicit_roles.do_not_fix

Valeur	Résultat
Faux	Ajouter snc_internal rôle en mémoire et en sys_user_has_role
Vrai	Ne pas ajouter snc_internal rôle dans la mémoire ou sys_user_has_role

Pour exclure snc_internal rôle pour certains utilisateurs, utilisez la propriété glide.security.explicit_roles.ignore.snc_internal.exclude_role_list .

Conseil :
Pour revenir au comportement précédent de glide.security.explicit_roles.do_not_fix, utilisez la propriété glide.security.explicit_roles.do_not_fix_in_memory .

Fournir l'accès aux tables aux utilisateurs externes

Vous pouvez donner accès à une table à des utilisateurs externes en ajoutant un rôle à la table qui hérite du rôle snc_external. Pour plus d'informations, consultez Provide external users access to a table .

La méthode hasRoles()

La méthode hasRoles() est toujours disponible, mais elle est déconseillée dans la version Geneva. Utilisez plutôt la méthode hasRole(nom de rôle).

Si vous utilisez la méthode hasRoles(), notez les changements suivants :

- Cette méthode exclut automatiquement le rôle snc_internal par défaut lorsqu'elle vérifie les rôles. Cela signifie que si un utilisateur possède uniquement le rôle snc_internal, la méthode hasRoles() renvoie toujours la valeur **faux**.
- Si l'utilisateur possède le rôle snc_external, la méthode renvoie la valeur **faux** car l'instance considère que les utilisateurs externes n'ont pas de rôle.

Exclusion mutuelle : snc_external contre snc_internal

ServiceNow AI Platform empêche les utilisateurs d'avoir le rôle snc_external et le rôle snc_internal à la fois. L'application ServiceNow AI Platform applique cette exclusion mutuelle partout dans le système et saisit des messages d'erreur dans les journaux pour chaque conflit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les ACL peuvent avoir les deux rôles si les ressources ACL doivent être accessibles à tous les utilisateurs.

Exemple : ajout de rôles explicites à un utilisateur (collision directe) :

1. Affectez à l'utilisateur Abel Tuter le rôle snc_internal.
2. Affectez à l'utilisateur Abel Tuter le rôle snc_external.

Résultat : l'ajout du rôle snc_external échoue car Abel Tuter a déjà le rôle snc_internal.

Exemple : ajout de deux rôles explicites à un groupe (collision directe) :

1. Considérez un groupe appelé groupe de tests qui n'a actuellement aucun rôle explicite affecté au groupe.
2. Ajoutez Abel Tuter au groupe de tests.
3. Ajoutez le rôle snc_external au groupe de tests.

Résultat : l'ajout du rôle snc_external échoue car Abel Tuter a déjà le rôle snc_internal et ne peut pas avoir les deux rôles.

Exemple : ajout d'un rôle explicite à un groupe dans lequel un membre du groupe a déjà le rôle explicite en conflit (collision indirecte) :

1. Affectez à l'utilisateur Abel Tuter le rôle snc_internal.
2. Considérez un groupe appelé groupe de tests qui n'a actuellement aucun rôle explicite affecté au groupe.
3. Ajoutez Abel Tuter au groupe de tests.
4. Ajoutez le rôle snc_external au groupe de tests.

Résultat : l'ajout du rôle snc_external au groupe échoue, car Abel Tuter hérite du rôle snc_external en appartenant au groupe. Les deux rôles explicites seront affectés au même utilisateur, ce qui n'est pas autorisé.

Pour d'autres exemples, consultez la table suivante :

Rôle	Tentative d'action	Résultat
Collision directe		
L'utilisateur a le rôle snc_internal.	Ajoutez le rôle snc_external.	L'action est abandonnée.
L'utilisateur a le rôle snc_external.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
L'utilisateur n'a pas de rôle explicite.	Ajoutez les rôles snc_external et snc_internal.	Le rôle est ajouté.
L'utilisateur a les deux rôles explicites (collision existante).	Ajoutez l'utilisateur à un groupe sans rôles.	L'action est abandonnée.
Un rôle qui n'est associé à aucun	Ajoutez le rôle snc_external.	L'action est abandonnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle	Tentative d'action	Résultat
utilisateur a le rôle snc_internal.		
Un rôle qui n'est associé à aucun utilisateur contient le rôle snc_internal.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
Un rôle contient les deux rôles explicites (collision existante).	Ajoutez le rôle à un utilisateur, un rôle ou un groupe.	L'action est abandonnée.
Un groupe sans membre a le rôle snc_internal.	Ajoutez le rôle snc_external.	L'action est abandonnée.
Un groupe sans membre a le rôle snc_external.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
Un groupe sans membre n'a aucun rôle.	Ajoutez les rôles snc_external et snc_internal.	Le rôle est ajouté.
Collision indirecte		
Confinement de rôle avec collision	1. Accordez un rôle appelé Rôle de test à un utilisateur avec le rôle snc_internal. 2. Ajoutez le rôle snc_external au rôle de test.	L'action est abandonnée.
Confinement de rôle sans collision	1. Accordez un rôle appelé Rôle de test à un utilisateur sans rôle. 2. Ajoutez le rôle snc_external au rôle de test.	Le rôle est ajouté à la fois à l'utilisateur et au rôle de test.
Confinement de groupe avec collision	1. Ajoutez un utilisateur qui a le rôle snc_internal à un groupe appelé Groupe de tests 2 (enfant du groupe de tests 1). 2. Ajoutez le rôle snc_external au groupe de tests 2. 3. Ajoutez le rôle snc_external à un groupe parent appelé Groupe de tests 1 (parent du groupe de tests 2).	L'action est abandonnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle	Tentative d'action	Résultat
Confinement de groupe sans collision	1. Ajoutez un utilisateur sans rôle à un groupe appelé Groupe de tests 2 (enfant du groupe de tests 1). 2. Ajoutez le rôle snc_external ou snc_internal au groupe de tests 1 (parent du groupe de tests 2).	Le rôle est ajouté au groupe parent, au groupe enfant et à l'utilisateur.
Confinement de groupe et confinement de rôle avec collision	Ajoutez contains_external au groupe de tests 1, le parent du groupe de tests 2.	Le groupe de tests 1 et le groupe de tests 2 obtiennent tous les deux contains_external, mais n'obtiennent pas explicitement le rôle snc_external.
	Ajoutez le rôle snc_internal au groupe de tests 2, l'enfant du groupe de tests 1.	L'action est abandonnée.
Changement de groupe parent plus confinement de groupe	1. Supprimez le groupe de tests 1 en tant que parent du groupe de tests 2. 2. Ajoutez le rôle snc_internal au groupe de tests 1. 3. Ajoutez le rôle snc_external au groupe de tests 2. 4. Dans le groupe de tests 2, définissez le groupe de tests 1 en tant que groupe parent et enregistrez.	L'action est abandonnée. Répétez pour les groupes déjà imbriqués, avec la même attente.

La cause d'une action abandonnée s'affiche dans le message d'erreur et doit être traitée avant la réussite d'une autre tentative.

Pour les tickets directs, tels que l'ajout d'un rôle explicite à un utilisateur individuel, vérifiez quel rôle explicite l'utilisateur doit avoir. Si l'utilisateur a un rôle explicite erroné, il doit d'abord être supprimé, puis le rôle explicite correct doit être ajouté.

Pour les incidents indirects, tels que l'ajout d'un rôle explicite à un groupe (afin qu'un membre du groupe ait les deux rôles explicites), évaluez si cet utilisateur doit être dans le groupe. Déterminez également si le groupe doit recevoir le rôle explicite, y compris tout héritage par la hiérarchie de groupe et la confinement des rôles.

Notez que ServiceNow AI Platform rapporte uniquement la première collision potentielle rencontrée. Si des tentatives répétées continuent d'échouer après la correction, avec une nouvelle cause première à chaque fois, réévaluez l'interdépendance utilisateur/groupe/rôle pertinente de façon plus étendue. Vous devrez peut-être repenser la façon dont les groupes et les conteneurs de rôles sont structurés.

Demander des rôles explicites

Activez Rôles explicites en demandant le module d’extension Rôles explicites (com.glide.explicit_roles) via Catalogue de Now Support services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

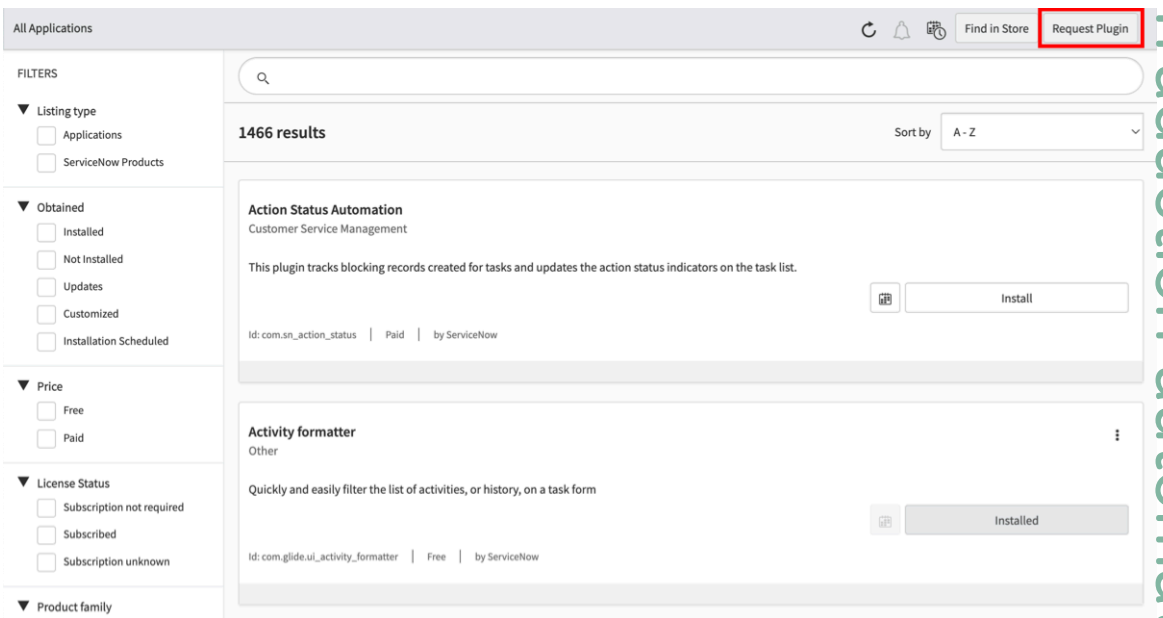
Avant de commencer

Rôle requis : admin

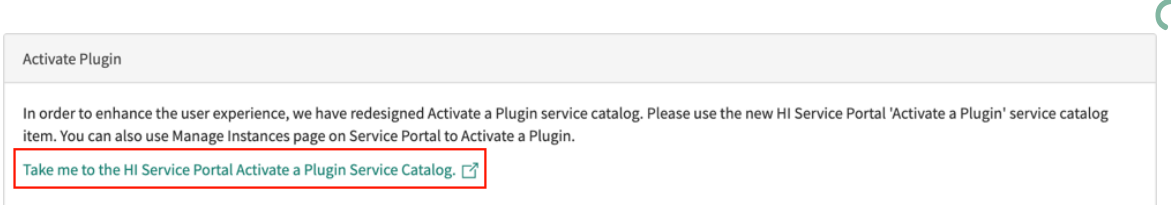
> **Important :**
> Activez ce module d'extension pendant une fenêtre de maintenance ou lorsque peu d'utilisateurs sont connectés. Les utilisateurs actuellement connectés lorsque le module d'extension est activé ne se verront pas attribuer dynamiquement le rôle snc_internal. Les utilisateurs doivent plutôt se déconnecter et se reconnecter pour se voir affecter le rôle snc_internal. Une fois le module d'extension activé, vous pouvez ajouter ou supprimer les rôles snc_internal et snc_external à tout moment pour changer les droits des utilisateurs.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

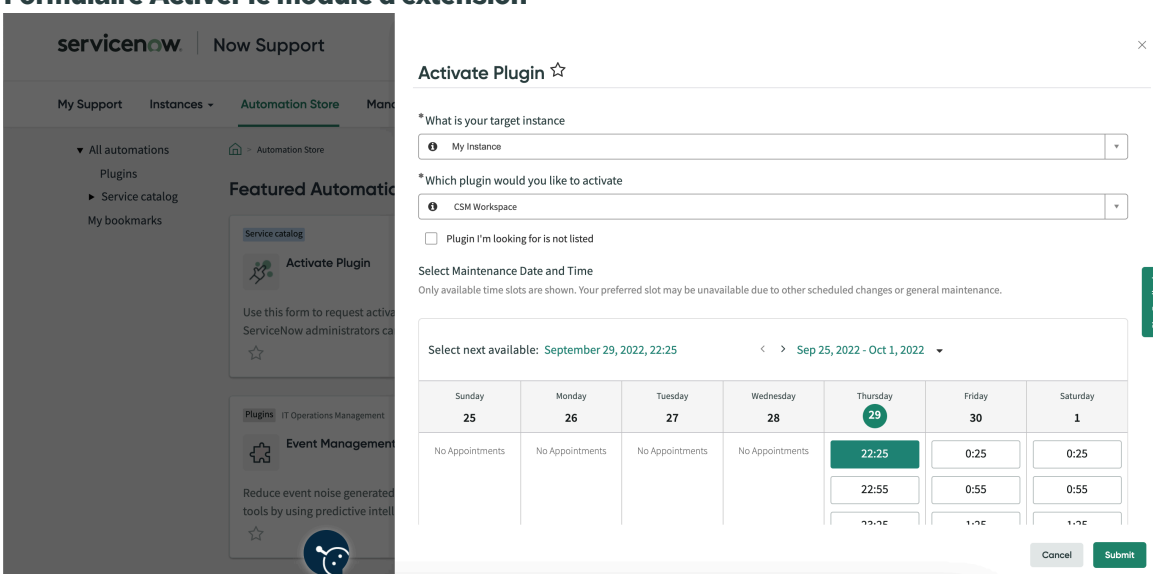
Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Soumettre**.
   Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Rôles à privilèges élevés

Les rôles à privilèges élevés exigent que vous acceptiez manuellement la responsabilité de l'utilisation du rôle avant de pouvoir accéder à ses fonctionnalités.

Par défaut, vous ne disposez pas de rôles de privilèges élevés lors de la connexion. Vous devez vous élever manuellement au privilège du rôle. Un rôle de privilège élevé ne dure que la durée de votre session utilisateur. Le délai d'expiration de la session ou la déconnexion supprime le rôle.

Vous pouvez désigner n'importe quel rôle comme un rôle de privilège élevé, puis affecter ce rôle à un ou plusieurs utilisateurs. Faites-le lorsque vous souhaitez empêcher les utilisateurs d'accéder aux droits accordés par le rôle immédiatement après la connexion. Vous pouvez désigner le rôle de privilège sur le formulaire Rôle. Consultez Créer un rôle pour obtenir des instructions.

Pour utiliser un rôle élevé, vous devez remplir les conditions suivantes :

- Le rôle élevé doit vous être affecté.
- Vous devez vous élever manuellement à un rôle élevé spécifique pour obtenir ses privilèges, même si vous êtes déjà élevé à un deuxième rôle élevé qui contient le premier rôle élevé.

  Par exemple, si un rôle élevé A contient un rôle élevé B, même si vous êtes élevé au rôle A, vous devez quand même être élevé au rôle B pour obtenir ses privilèges.

Le rôle administrateur

Pour accorder le rôle administrateur à un utilisateur, celui-ci doit également disposer du rôle administrateur. Par exemple, un utilisateur ayant uniquement le rôle user_admin ne peut pas accorder le rôle administrateur à d'autres utilisateurs.

- Les utilisateurs non-administrateurs ne peuvent pas ajouter d'utilisateur à un groupe qui contient le rôle administrateur.
- Pour accorder le rôle security_admin à un utilisateur, celui-ci doit également disposer du rôle administrateur et doit s'élever au rôle security_admin avant d'accorder le rôle security_admin à d'autres utilisateurs. Un utilisateur disposant uniquement du rôle administrateur ne peut pas accorder le rôle security_admin à d'autres utilisateurs.
- Un utilisateur sans le rôle security_admin ne peut pas ajouter un utilisateur à un groupe qui contient le rôle security_admin.

Avertissement :
L'utilisation de privilèges élevés sur un rôle administrateur n'est pas prise en charge. Au lieu de cela, exigez des administrateurs qu'ils élèvent manuellement, consultez Forcer les administrateurs à élever manuellement

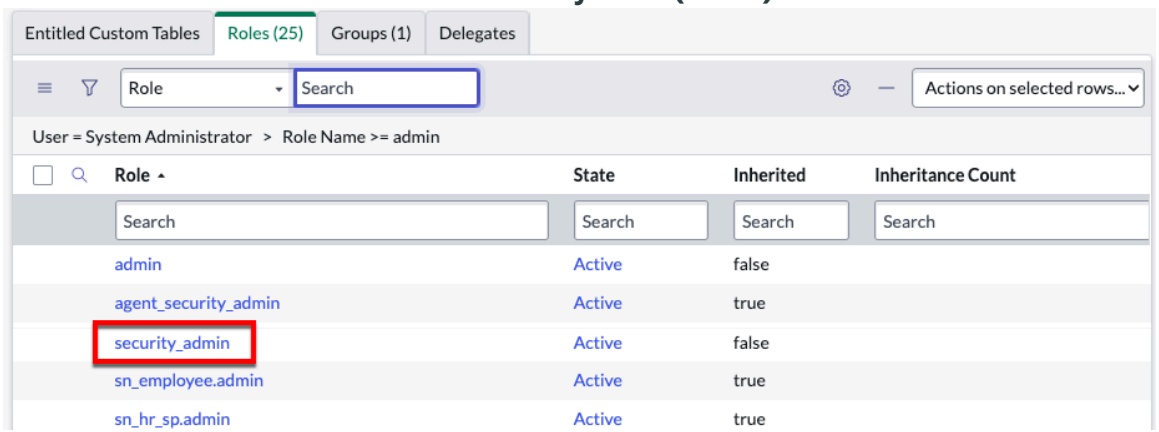
Le rôle security_admin

Dans le système de base, le rôle security_admin est le seul rôle qui dispose de privilèges élevés. Ce rôle est automatiquement affecté à l'utilisateur qui est l'utilisateur administrateur système (admin) par défaut. Il donne accès aux ACL et aux paramètres de sécurité élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles affectés à l'utilisateur administrateur système (admin)



Remarque :
Pour voir ce rôle, vous devez d'abord accéder au rôle security_admin. Si vous êtes connecté en tant qu'utilisateur administrateur système (admin) uniquement, vous ne pouvez pas voir l'enregistrement security_admin dans la liste des rôles.

Security_admin rôle

Le rôle security_admin est un rôle à privilèges élevés fourni avec des paramètres de sécurité élevée qui permet aux utilisateurs de créer et de modifier des contrôles d'accès et de modifier des paramètres de sécurité élevée.

Dans le système de base, seul l'utilisateur administrateur système (admin) par défaut dispose du rôle security_admin. Étant donné qu'elle nécessite des privilèges élevés, l'utilisateur administrateur n'a pas ce rôle lors de la connexion. Après l'élévation des privilèges, l'utilisateur administrateur dispose du rôle security_admin pour la durée de la session utilisateur. Consultez Accéder à un rôle privilégié pour plus d'informations.

Pour maintenir une sécurité élevée, le rôle security_admin nécessite des privilèges élevés. Limitez les utilisateurs et les groupes auxquels vous affectez ce rôle.

Accéder à un rôle privilégié

L'administrateur système de base peut s'élever à un rôle privilégié pour avoir accès aux fonctionnalités des paramètres de sécurité élevée.

Avant de commencer

Rôle requis : admin

Remarque :
Si vous accordez le rôle d'administrateur à des utilisateurs supplémentaires, ils ne peuvent pas accéder à un rôle privilégié. Seul l'administrateur système de base peut élever au niveau supérieur.

Procédure

1. Dans le cadre de la bannière, cliquez sur votre image ou cliquez sur vos initiales si vous n'avez pas d'image téléchargée.
2. Sélectionnez **Élever les rôles**.
   Une boîte de dialogue s'affiche qui contient les rôles disponibles pour l'élévation.
3. Sélectionnez les rôles élevés à affecter et cliquez sur **OK**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce rôle accorde à l'utilisateur des privilèges élevés sur toutes les ressources contrôlées par le rôle pour le reste de la session. Lorsque l'utilisateur se déconnecte, les privilèges élevés prennent fin avec la session, mais peuvent être rétablis à la prochaine connexion.

4. Mettez fin à l'élévation du rôle en revenant à la boîte de dialogue de l'étape 2 et en désélectionnant le rôle.

Forcer les administrateurs à élever manuellement

Une propriété est disponible pour forcer tous les utilisateurs ayant le rôle d'administrateur à sélectionner manuellement le rôle auquel ils souhaitent s'élever.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Connectez-vous en tant qu'administrateur.
2. Élevez votre rôle à security_admin.
3. Accédez à **sys_properties.list**.
4. Recherchez et sélectionnez la `glide.security.strict_elevate_privilege` propriété.
5. Définissez le champ Valeur sur **vrai** et cliquez sur **Soumettre**.

Résultats

Lorsque l'utilisateur se connecte, une boîte de dialogue s'affiche lui permettant de sélectionner le rôle auquel il peut s'élever.

Connexions et informations d'identification

Les informations d'identification et de connexion sont nécessaires pour accéder à un ordinateur ou à un appareil réseau pour Découverte, Mappage des services et Gestion cloud, ou pour travailler avec Orchestration. Lors de l'ajout de contenu à Share ou AppStore, vous pouvez configurer les connexions et les informations d'identification pertinentes pour votre environnement sans modifier le contenu créé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Explorer



En savoir plus sur les informations d’identification.

Configurer



Configurez les informations d’identification.

Référence



Obtenez des détails sur les informations d’identification.

Dépannage



Découvrez comment résoudre les problèmes de connexion et d’informations d’identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer les informations d'identification, les connexions et les alias

Toutes les intégrations d'applications dans le utilisent des connexions, des informations d'identification ServiceNow AI Platform et des alias pour permettre aux applications d'accéder aux ressources.

Avant de pouvoir exécuter une intégration d'application dans le , vous devez créer et configurer les ServiceNow AI Platform informations de connexion, les informations d'identification correspondantes et ajouter un alias. Pour comprendre comment ServiceNow définit ces termes :

Connexion

Une *connexion* est une intégration à un système, telle qu'une adresse IP ou un point de terminaison avec des protocoles. Elle contient des détails spécifiques, tels que des détails de base de données, lors de l'intégration à une base de données.

Informations d'identification

Les *informations d'identification* correspondent aux données d'authentification requises pour établir la connexion, telles qu'un identifiant et un mot de passe.

Alias

Un *alias* est une convention de dénomination, ou balise, qui se lie à un ensemble de connexions ou d'informations d'identification sur votre instance. Un alias contient les informations de connexion et d'identification nécessaires pour effectuer une intégration d'application. Plutôt que de saisir ces informations à chaque intégration, vous pouvez utiliser un alias. Par exemple, vous pouvez désigner un alias pour héberger vos informations d'identification en matière d'assurance qualité, de développement et de production pour la même intégration d'application. L'alias résout l'intégration d'application pour chaque environnement.

Le ServiceNow AI Platform distingue différents types d'alias :

Alias d'informations d'identification

Cet alias s'associe uniquement aux données d'informations d'identification et se résout pendant l'exécution.

Alias de connexion et d'informations d'identification

Cet alias associe les informations de connexion et les données d'identification requises pour terminer l'intégration et se résout pendant l'exécution.

Dans les alias de connexion et d'informations d'identification, vous pouvez également créer des alias supplémentaires appelés *alias enfants*. Les alias enfants vous permettent de créer plusieurs connexions au sein d'une même intégration d'application. Lorsque vous créez un alias enfant, l'alias sous lequel vous l'avez créé devient un *alias parent*. Alors que les alias enfants héritent des propriétés de leur alias parent, les alias enfants portent leurs propres informations de connexion et d'identification.

Avantages de l'utilisation des connexions, des informations d'identification et des alias

- Emplacement central pour stocker et gérer les informations d'identification vers un service externe
- Définir une fois et réutiliser pour plusieurs fonctionnalités de plateforme
- Réduire la configuration des autres fonctionnalités de la plateforme

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Autoriser les non-administrateurs à utiliser des connexions et des informations d'identification prédéfinies
- Sécurité accrue

Fonctionnalités utilisant des connexions, des informations d'identification et des alias

Les fonctionnalités suivantes utilisent des connexions, des informations d'identification et des alias :

- Concepteur de flux
- Centre d'intégration
- Gestion cloud
- Découverte
- Orchestration
- Mappage des services

Vous pouvez configurer des alias sur le de l'une ServiceNow AI Platform des deux façons suivantes :

- À l'aide du Connexions et informations d'identification module. Consultez Créer un alias de connexion et d'informations d'identification.
- Dans le tableau de bord Connexions de Centre d'intégration. Voir Ajouter une connexion .

> **Remarque :**
> Centre d'intégration nécessite un abonnement distinct. Pour plus d'informations, consultez Demande Centre d'intégration .

Synchronisation des informations d'identification sur les serveurs MID

Chaque *serveur MID*de votre réseau synchronisé avec l'instance conserve une copie de chaque information d'identification que vous créez. Le serveur MID (Management, Instrumentation, and Discovery) est une application Java qui permet la communication et le mouvement de données entre une instance ServiceNow et des applications, sources de données et services externes. Cette synchronisation accélère la lecture des informations d'identification lorsque les applications aiment Découverte ou Mappage des services doivent accéder à plusieurs appareils sur le réseau. Les MID Servers se synchronisent lorsqu'ils trouvent une `credentials_reload` tâche dans la file d'attente ECC. La tâche de rechargement demande au serveur MID d'effectuer un appel SOAP vers l'instance pour obtenir la liste complète des informations d'identification dans la table Informations d'identification [discovery_credentials], y compris toutes les valeurs de champ. Pour plus d'informations, consultez Serveur MID .

La réponse SOAP que votre instance envoie à chaque serveur MID comprend également des champs personnalisés que vous avez ajoutés à n'importe quel formulaire d'informations d'identification que vous avez personnalisé. Si vous avez ajouté des champs de référence, les données de la table référencée sont également envoyées dans le cadre de la réponse SOAP. Cela peut entraîner des problèmes de performances lorsque la synchronisation des informations d'identification se produit avec plusieurs serveurs MID. Pour contrôler cela, ajoutez manuellement ces propriétés à la table Propriétés système [sys_properties] :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour modifier les valeurs de ces propriétés, ajoutez-les à la table Propriétés système [sys_properties]. Si vous ne les ajoutez pas, le système utilise la valeur par défaut.

Propriété	Description
com.snc.credentials_user_fields	Inclut tous les champs personnalisés dans la synchronisation des informations d'identification. Définissez cette propriété sur faux si vous ne souhaitez pas inclure les champs que vous avez ajoutés aux formulaires d'informations d'identification. • **Type** : vrai | faux • **Valeur par défaut** : true
com.snc.credentials_recursion_depth	Définit le nombre de tables à parcourir lorsque le mécanisme de synchronisation des informations d'identification collecte les champs des tables de référence. Réduisez ce nombre si vous rencontrez des problèmes de performances et si vous avez des formulaires d'informations d'identification personnalisés qui incluent des champs de référence vers des tables qui ont également des champs de référence. • **Type** : nombre entier • **Valeur par défaut** : 3

Protéger les champs d'application pour les informations d'identification et les connexions

Vous pouvez classer certains types d'enregistrements Connexion et informations d'identification comme appartenant à un champ d'application et leur étendre des protections de champ d'application. Ces politiques de champ d'application protègent les enregistrements que vous créez dans une table et empêchent les interactions avec des enregistrements privés à un autre champ d'application.

Un champ **Application** est disponible dans les tables Connexion [sys_connection] et Informations d'identification de détection [discovery_credentials] pour associer ces types d'enregistrements à des champs d'application spécifiques. Il n'est pas visible sur les formulaires d'interface utilisateur dans Yokohama, mais vous pouvez facilement l'y ajouter. Pour en savoir plus sur ces types d'enregistrements et sur l'ajout du champ à leurs formulaires d'interface utilisateur, voir :

- Mise en route des connexions
- Introduction aux informations d'identification
- Alias d'informations d'identification pour Découverte
- Configurer la mise en page du formulaire

Restreindre l'utilisation d'un enregistrement Connexion et informations d'identification à un champ d'application spécifique est primordial pour gérer les applications qui nécessitent une sécurité appliquée. Ces applications comprennent Prestation de services RH ou Opérations de sécurité Les enregistrements de connexion et d'informations d'identification créés dans les applications administrées incluses dans le périmètre ne sont pas visibles par les utilisateurs administrateurs. L'association d'un enregistrement de connexion et d'informations d'identification à un périmètre d'application spécifique offre les protections suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Applique des règles de liste de contrôle d'accès (ACL) aux champs d'application restreints. Pour en savoir plus sur les ACL incluses dans le périmètre, consultez Règles de la liste de contrôle d'accès.

  Remarque :
  Certaines applications utilisant l'administration de champ d'application et la sécurité renforcée peuvent nécessiter une configuration supplémentaire. Pour en savoir plus, voir Gérer les rôles RH

- Protège les enregistrements lorsqu'ils sont interrogés à l'aide d'un script. Si vous effectuez une requête à partir du champ d'application global et que l'enregistrement de connexion et d'informations d'identification se trouve dans un champ d'application protégé, il n'apparaît pas dans la requête, sauf si vous y avez accès.

Vous pouvez personnaliser et accorder l'accès aux enregistrements restreints par requête à l'aide de l'accès restreint pour l'appelant. Pour en savoir plus, consultez Paramètres de privilège d'accès restreint pour l'appelant . Les restrictions de définition du champ d'application s'appliquent également à toutes les tables enfants des tables Connexion [sys_connection] et Informations d'identification de découverte [discovery_credentials]. Les champs vides et les autres champs d'application ne sont pas restreints.

Remarque :
Les protections de champ d'application ne sont activées que pour des champs d'application sécurisés spécifiques afin d'éviter toute confusion lors de la configuration de nouveaux enregistrements. Si quelqu'un établit une connexion dans son périmètre d'application inclus dans le périmètre, il n'y a pas de restriction automatique du périmètre.

Séparation de domaine et Informations d'identification et connexions

L'application Séparation de domaine est prise en charge dans Informations d'identification et connexions. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

Les informations d'identification sont liées à diverses ServiceNow fonctionnalités qui accèdent à des systèmes en dehors de l'instance. Les informations d'identification suivent la séparation de domaine liée à la fonctionnalité qui utilise les informations d'identification.

Les connexions sont des informations spécifiques au protocole qui font référence à un hôte cible en dehors de l'instance. Une connexion peut spécifier le domaine pour exécuter une activité.

Fonctionnement de Séparation de domaine dans Informations d'identification et connexions

Les informations d'identification accèdent à des ressources en dehors de l'instance et sont utilisées par Découverte , Orchestration , Mappage des services , et Cloud Provisioning and Governance Applications. Ces informations d'identification ne sont pas liées à un domaine spécifique. Elles peuvent être liées à une application, puis suivre la séparation de domaine utilisée par l'application. Les informations d'identification peuvent également être affectées à un serveur MID , puis suivre la séparation de domaine spécifiée par la Serveur MID configuration.

Les connexions accèdent à un hôte cible à l'aide d'une connexion *JMS*, *JDBC* ou *HTTP(s*). Vous pouvez spécifier un domaine global ou spécifique auquel appartient la connexion.

Information associée

Séparation de domaine pour les fournisseurs de services

Modèles de configuration de connexion et d'informations d'identification

Permettez aux utilisateurs ayant les rôles administrateur et flow_designer de configurer des intégrations de spoke avec des systèmes tiers à l'aide d'un formulaire unique personnalisable.

Par exemple, vous pouvez configurer une intégration OAuth, qui enregistre un fournisseur OAuth, génère un jeton et crée des enregistrements de connexion et d'informations d'identification. Un concepteur ou développeur d'action peut utiliser un modèle de configuration pour configurer le spoke à un emplacement unique et le système crée les enregistrements associés.

Avantages

Les modèles de configuration permettent :

- Les administrateurs ou les concepteurs de flux pour configurer des intégrations complexes à l'aide d'un formulaire unique.
- Permettre aux développeurs de définir des valeurs statiques dans une intégration, ce qui simplifie le processus de configuration pour les administrateurs et les concepteurs de flux.

Types d'informations d'identification pris en charge

Vous pouvez créer des modèles de configuration pour les intégrations avec ces types d'informations d'identification :

- Authentification de base
- Clé API

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Type d’attribution titulaire OAuth JWT
- Type d’accord du code d’autorisation OAuth
- Authentification personnalisée

Composants de modèles de configuration

Modèle de données par défaut

Définit les informations statiques qui s'appliquent à chaque intégration. Par exemple, vous pouvez définir l'API et l'URL du jeton si la valeur s'applique à chaque intégration.

Modèle de données dynamiques

Définit les informations que l'utilisateur doit renseigner pour configurer l'intégration. Par exemple, vous pouvez ajouter des paires de valeurs clés de nom d'utilisateur et de mot de passe pour collecter des valeurs définies par l'utilisateur.

Script de post-traitement

Crée les enregistrements supplémentaires requis par l'intégration. Par exemple, si votre spoke inclut des tables personnalisées, vous pouvez créer des enregistrements dans ces tables en fonction de l'entrée de l'utilisateur dans le modèle de configuration. Ce script s'exécute une fois que les enregistrements de connexion et d'informations d'identification sont créés.

Script de pré-édition

Pré-remplit les champs personnalisés de la section **Informations supplémentaires** lorsque vous modifiez une connexion existante. Le pré-remplissage des champs personnalisés vous permet d’afficher la valeur actuelle associée au champ personnalisé.

Action de test

Vous permet de tester une connexion directement à partir d’une action d’intégration dans la vue de flux de Studio de workflow. L’action de test utilise une définition d’action pour tester l’alias auquel le modèle est actuellement attaché. Pour plus de détails, voir Create a test action to test a connection alias from a configuration template .

Données de démonstration

La table Modèles de connexion et d’informations d’identification [sys_alias_templates] comprend des exemples de modèles illustrant comment configurer des modèles pour les types d’authentification courants. Utilisez ces exemples comme guide lors de la création du vôtre.

Configurer un modèle pour le type d’attribution titulaire OAuth JWT

Cet exemple de modèle de configuration configure les enregistrements d’informations d’identification et de connexion à l’aide du type d’attribution JWT Bearer pour authentifier les demandes adressées à Docusign.

Modèle de données par défaut

Chaque élément de niveau supérieur dans le modèle de données par défaut crée un enregistrement associé. Le modèle comprend les sections suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Informations d'identification : crée un enregistrement dans la table Informations d'identification.
- Connexion : crée un enregistrement dans la table Connexions [sys_connection] et tous les enregistrements de connexion associés.
- Supplémentaire : Crée éventuellement des enregistrements dans une table personnalisée. Le script de post-traitement indique au système ce qu'il doit faire de ces enregistrements.

L'exemple suivant crée les enregistrements requis pour l'authentification de type d'attribution titulaire OAuth JWT.

```
{
 "credential": {
  "oauth_entity": {
   "oauth_entity_profile": [
    {
     "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
     "name": "Docusign Profile",
     "default": true,
     "oauth_entity_profile_scope": [
      "users:read.email"
     ]
    }
   ],
   "code_challenge_method": "S256",
   "type": "consumer",
   "oauth_entity_scope": [
    {
     "oauth_entity_scope": "users:read.email",
     "name": "email"
    }
   ],
   "client_id": "<provider-client-id>",
   "use_mutual_auth": false,
   "revoke_token_url": "https://<provider-domain-name>.com/oauth2/revoke",
   "default_grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
   "public_client": false,
   "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
   "name": "Docusign Spoke OAuth",
   "client_secret": "<provider-client-secret>",
   "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
   "token_url": "https://<provider-domain-name>.com/oauth2/token",
   "redirect_url": "https://<instance-name>.service-now.com/oauth_redirect.do"
  },
  "jwt_provider": {
   "jwt_keystore_aliases": {
    "kid": "<provider-key-id>",
    "name": "Docusign Spoke JWT Key",
    "signing_keystore": "<signing-keystore-sys-id>",
    "signing_algorithm": "rsa_256",
    "signing_key_password": "password"
   },
   "jwt_claim_validation" : [ {
    "name" : "iss",
    "is_standard" : true,
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
      "data_type" : "string",
      "value":"<docusign-iss-claim>"
    }, {
      "name" : "sub",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
    "name": "Docusign Spoke JWT Provider",
    "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
  },
  "name": "Docusign Spoke Credential",
  "table": "oauth_2_0_credentials"
 },
 "connection": {
  "use_mid": false,
  "connection_url": "https://<provider-domain-name>.com",
  "name": "Docusign Spoke Connection",
  "table": "http_connection"
 },
"additional":{
  "docusign_account_name": "<docusign-account-name>",
  "docusign_account_email": "<docusign-account-email>"
}
}
```

Schéma de données dynamique

Le schéma de données dynamiques définit ce que l'utilisateur voit lorsqu'il crée un alias de connexion et d'informations d'identification et collecte ses entrées. Utilisez la syntaxe de remontée pas à pas pour mapper l'entrée de l'utilisateur aux champs créés dans le modèle de données par défaut. Par exemple, `connection_fields` mappe l'entrée de l'utilisateur au champ `connection_url` dans l'objet de `connexion` créé par le modèle de données par défaut.

```
{
 "connection_fields": [
  {
   "name": "connection.connection_url",
   "label": "Connection URL",
   "type": "text",
   "defaultValue": "https://demo.docusign.net",
   "hint": "Connection URL for Docusign"
  }],
"additional_fields":[
  {
   "name": "additional.docusign_account_id",
   "label": "Docusign Account Number",
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "type": "text",
    "hint": "Docusign Account Number"
   },
   {
    "name": "additional.docusign_account_name",
    "label": "Docusign Account Name",
    "type": "text",
    "hint": "Name to identify the Docusign account"
   },
   {
    "name": "additional.docusign_account_email",
    "label": "Docusign Account Email",
    "type": "text",
    "hint": "Docusign Account Email"
   }
 ],
 "credential_fields": [
   {
    "name": "credential.oauth_entity.client_id",
    "label": "OAuth Client ID",
    "type": "text",
    "hint": "Client ID for Docusign"
   },
   {
    "name": "credential.oauth_entity.redirect_url",
    "label": "OAuth Redirect URL",
    "type": "text",
    "defaultValue": "https://<instance-name>.service-now.com/oauth_redirect.do",
    "hint": "Callback URL for Docusign"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[0].value",
    "label": "Issuer (iss) Claim value",
    "type": "text",
    "hint": "The integrator key (also known as client ID) of the application"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[1].value",
    "label": "Subject (sub) Claim value",
    "type": "text",
    "hint": "The user ID of the user to be impersonated"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[2].value",
    "label": "Audience (aud) Claim value",
    "type": "text",
    "defaultValue": "account-d.docusign.com",
    "hint": "The URI of the authentication service instance to be used e.g.
account.docusign.com"
   },
   {
    "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
    "label": "Key ID (kid)",
    "type": "text",
    "hint": "Indicates which key was used to secure the JWS"
   },
   {
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
   }
  ]
}
```

Script de post-traitement

Le script de post-traitement suivant mappe l'entrée de l'utilisateur aux champs de la table sn_docusign_spoke_accounts.

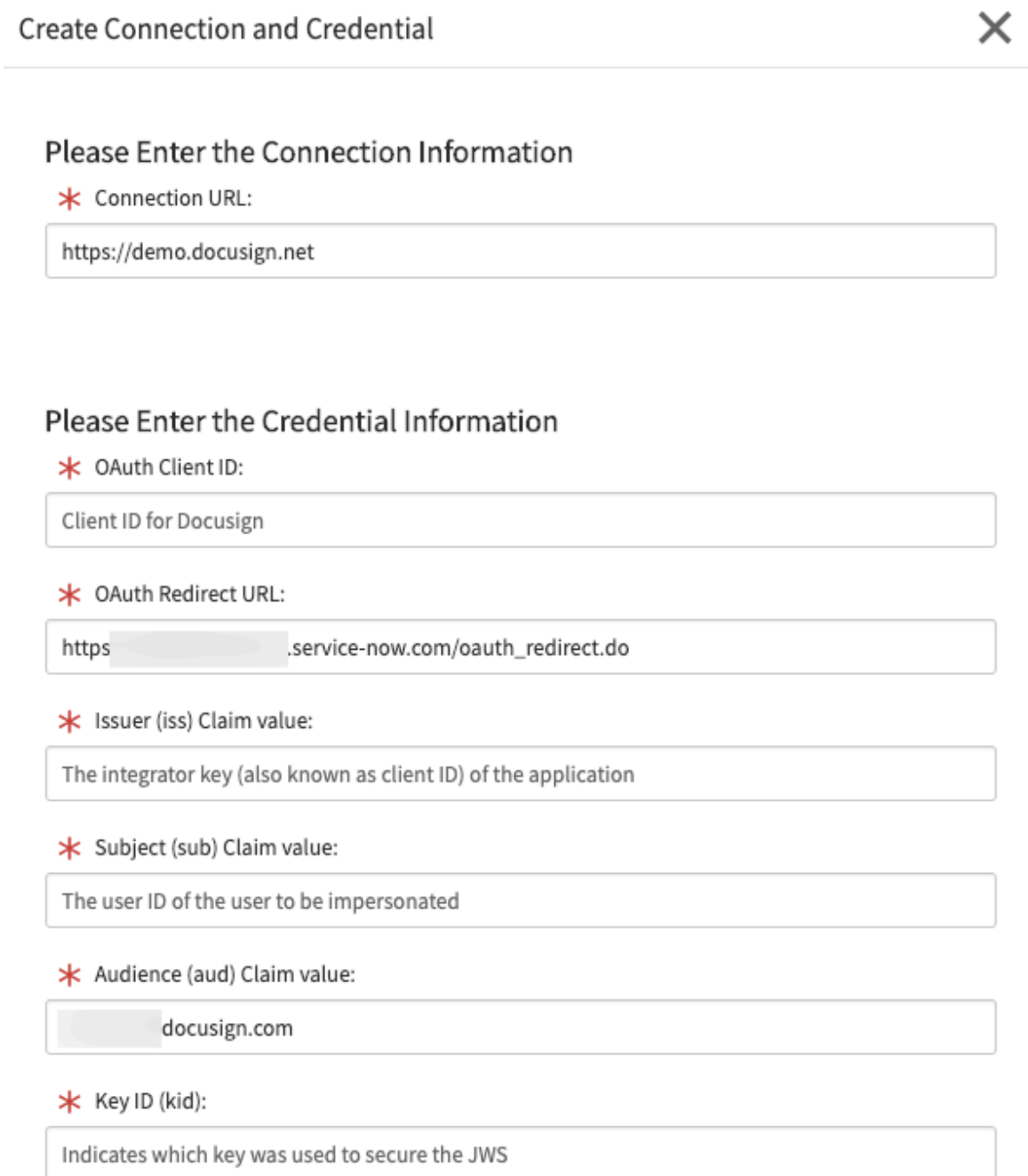
```
(function execute(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
   accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
   accountGR.setValue("alias", aliasId);
   accountGR.setValue("email", jsonDynamicDataP["additional.docusign_account_email"]);
   accountGR.setValue("id", jsonDynamicDataP["additional.docusign_account_id"]);
   accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

Formulaire de configuration de connexion et d'informations d'identification Docusign résultant

Lorsque l'utilisateur accède à l'alias de connexion et d'informations d'identification Docusign associé et sélectionne **Créer une nouvelle connexion et de nouvelles informations d'identification**, la boîte de dialogue suivante s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Créer un modèle de configuration

Créez un modèle qui définit les entrées requises pour configurer un spoke. Définissez des paires clé-valeur statiques pour créer des enregistrements et définir des valeurs qui s'appliquent à chaque intégration. Définissez des paires clé-valeur dynamiques pour collecter des entrées utilisateur et définir des valeurs de champ qui peuvent varier. À l'aide de ce modèle, les administrateurs et les concepteurs de flux peuvent configurer le spoke à partir d'un formulaire unique.

Avant de commencer

Rôle requis : admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Centre d'intégration** > **Connexions et informations d'identification** > **Modèles de configuration**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez le type de modèle de configuration que vous souhaitez créer.
4. Dans le champ **Nom** , ajoutez un nom pour identifier le modèle.
5. Dans le champ **Modèle de données par défaut** , apportez les changements requis.

   Ce champ définit des informations statiques qui s'appliquent à chaque intégration. Par exemple, vous pouvez définir l'API et l'URL du jeton si la valeur s'applique à chaque intégration.

   Ces objets dans le modèle de données par défaut sont requis :

   - `informations d'identification` : crée un enregistrement d'informations d'identification avec les champs requis.
   - `connexion` : crée un enregistrement de connexion avec les champs requis. Accédez aux attributs de connexion à l'aide de l'objet enfant `extended_attributes` . Par exemple :

     ```
     "connection": {
             "extended_attributes": {
                "api_version": "v1"

             },
         "connection_url": "https://<provider-domain-name>.com",
         "name": "Spoke Connection",
         "table": "http_connection"
       }
     ```

   Vous pouvez utiliser l'objet `supplémentaire` pour configurer des données pour une table personnalisée et utiliser le script de post-traitement pour insérer les données dans la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Dans le modèle de données par défaut du type d'accord Code d'autorisation OAuth, les valeurs du `oauth_entity_profile_scope` et des clés `oauth_entity_scope` doivent correspondre. Dans l'exemple suivant, les deux clés ont la valeur `E-mail de l'utilisateur en lecture` .

```
"oauth_entity_profile": [
      {
       "grant_type": "authorization_code",
       "name": "<provider-name> Profile",
       "default": true,
       "oauth_entity_profile_scope": [
        "Read user's email"
       ]
      }
     ],
     "code_challenge_method": "S256",
     "type": "consumer",
     "oauth_entity_scope": [
      {
       "oauth_entity_scope": "Read user's email",
       "name": "email"
      }
     ],
```

6. Dans le champ **Schéma de données dynamique** , apportez les changements requis.

   Ce champ Définit les informations que l'utilisateur doit renseigner pour configurer l'intégration. Par exemple, vous pouvez ajouter des paires de valeurs clés de nom d'utilisateur et de mot de passe pour collecter des valeurs définies par l'utilisateur.

   Les champs du schéma de données dynamiques incluent ces propriétés :

   - `nom` : champ auquel l'entrée de l'utilisateur est mappée. Par exemple, pour mapper l'entrée de l'utilisateur au champ URL de connexion de l'enregistrement de connexion, saisissez `connection.connection_url`.
   - `étiquette` : l'étiquette de champ que l'utilisateur voit lorsqu'il termine le modèle.
   - `type` : type de champ. Assurez-vous que ce type de données correspond au type de données du champ avec lequel vous mappez la valeur.
   - `defaultValue` : facultatif. Valeur par défaut du champ. Si aucune valeur par défaut n'est fournie, l'indicateur s'affiche.
   - `conseil` : facultatif. Texte de conseil à afficher en l'absence de valeur par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous configurez un modèle pour l'authentification de type d'attribution titulaire OAuth JWT, vous pouvez souhaiter une entrée utilisateur pour une seule paire clé-valeur dans le tableau `jwt_claim_validation` . Vous pouvez faire référence à une seule paire clé-valeur dans le schéma de données dynamiques en vous référant à son index dans le tableau. Par exemple, votre modèle de données par défaut peut inclure cet extrait.

```
"jwt_claim_validation" : [ {
      "name" : "iss",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-iss-claim>"
    }, {
      "name" : "sub",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
```

Reportez-vous à la paire clé-valeur `iss` à l'aide de l'index de base zéro de l'élément : `credential.jwt_provider.jwt_claim_validation[0].value`.

7. **Facultatif :** Dans le champ **Script de post-traitement** , ajoutez un script qui c Crée les enregistrements supplémentaires requis par l'intégration. Par exemple, si votre spoke inclut des tables personnalisées, vous pouvez créer des enregistrements dans ces tables en fonction de l'entrée de l'utilisateur dans le modèle de configuration. Ce script s'exécute une fois que les enregistrements de connexion et d'informations d'identification sont créés.
   Le script de post-traitement a accès à ces objets globaux.

Objet global	Description
aliasId	Sys_id de l'enregistrement d'alias de la table Alias de connexion et d'informations d'identification [sys_alias].
connectionSysId	Sys_id de l'enregistrement de connexion créé par le modèle.
jsonDefaultData	Contenu JSON du champ **Modèle de données par défaut** au format chaîne.
jsonDynamicData	Contenu JSON du champ **Modèle de données dynamiques** au format Chaîne.

8. Dans le champ **Pré-modifier le script** , ajoutez un script pour pré-remplir les champs supplémentaires lorsque vous modifiez une connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce script renvoie un tableau d'objets. Chaque objet possède une paire nom-valeur pour renseigner les champs supplémentaires. Par exemple, si la connexion nécessite des champs qui se trouvent dans une table personnalisée, vous pouvez mapper ces champs à la table personnalisée.

Le **script de pré-édition** a accès aux objets globaux suivants :

Objet global	Description
aliasId	Sys_id de l'enregistrement d'alias de la table Alias de connexion et d'informations d'identification [sys_alias].
connectionSysId	Sys_id de l'enregistrement de connexion créé par le modèle.
jsonDefaultData	Contenu JSON du champ **Modèle de données par défaut** au format chaîne.
jsonDynamicData	Contenu JSON du champ **Modèle de données dynamiques** au format Chaîne.

Chaque objet du script possède les propriétés suivantes :

- `Nom` : nom du champ personnalisé pour spécifier la valeur dans la connexion.
- `value` : valeur que vous souhaitez mapper pour remplir le champ personnalisé. Vous pouvez mapper le champ à l'aide d'une fonction ou d'une variable, ou en le codant en dur.

Les types de données suivants sont pris en charge pour les champs :

Types de données pris en charge pour les champs

Type	Description
Texte	Valeur de chaîne.
Booléen	Zone de sélection. La sélection indique une valeur vrai et la désélection indique une valeur fausse.
Numéro	Valeur numérique.
Date	Valeur de date au format aaaa-mm-jj. Vous pouvez également utiliser l'objet GlideDate.
Choix	Liste de choix valides définis dans le champ **Schéma de données dynamique**.
Référence	GlideRecord valide.
Groupe de cases d'option	Regroupe qui contient un ensemble différent de champs. Ces groupes sont disponibles dans une liste déroulante lorsque vous modifiez une connexion. Les champs de chaque groupe s'affichent lorsque vous sélectionnez le groupe requis dans la liste déroulante. Par exemple, considérez la structure suivante du groupe de cases d'option défini dans le champ **Schéma de données dynamiques** : `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio",`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type	Description

	<pre>"groups": [{
	"name": "radio_group1",
	"label": "Radio Group 1",
	"fields": [{
	"name": "radio_field1",
	"label": "Radio Field 1",
	"type": "text",
	"defaultValue": "efgh",
	"mandatory": true
	}]
	}, {
	"name": "radio_group2",
	"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre>
	Pour cet exemple, vous pouvez utiliser l'extrait de code suivant pour comprendre comment les groupes de cases d'option sont utilisés dans le script à l'aide de la remontée pas à pas :
	<pre>{
	name: "radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value: gr.getValue(‘radio_groups’)
	}</pre>
	Pour plus d'informations sur l'utilisation de la remontée pas à pas, consultez Remontée pas à pas .

Conseil :
Si les valeurs préremplies n'apparaissent pas dans les champs lors de la modification d'une connexion, accédez à **Diagnostics du système** > **Débogage de session** > **Journal des débogages** pour diagnostiquer le problème.

9. **Facultatif :** Dans le champ **Action de test** , entrez le nom de l'action de test.
   La création d'une action de test vous permet de tester une connexion directement à partir d'une action d'intégration dans la vue de flux de Studio de workflow. L'action de test utilise une définition d'action pour tester l'alias auquel le modèle est actuellement attaché. Pour plus de détails, voir Create a test action to test a connection alias from a configuration template .
10. Ajoutez le modèle à un alias de connexion et d'informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Centre d'intégration** > **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.

b. Ouvrez l'enregistrement d'alias pour le spoke.

c. Dans le champ **Modèle de configuration** , cliquez sur l'icône de recherche.

d. Sélectionnez le modèle que vous avez créé dans la liste.

e. Cliquez sur **Mettre à jour**.

Résultats

Lorsque l'utilisateur accède à l'alias de connexion et d'informations d'identification associé et sélectionne **Créer une nouvelle connexion et de nouvelles informations d'identification**, une boîte de dialogue s'affiche pour collecter ses entrées. Si vous avez créé un modèle pour le type d'accord Code d'autorisation OAuth, vous pouvez également récupérer un jeton OAuth à partir de cette boîte de dialogue.

Que faire ensuite

Testez le modèle en accédant à l'alias de connexion et d'informations d'identification associé, puis en sélectionnant **Créer une nouvelle connexion et informations d'identification**. Vérifiez que la boîte de dialogue collecte les données attendues et crée les enregistrements requis dans le système.

Mise en route des connexions

Utilisez la table connexions pour configurer une connexion de base, JMS, JDBC ou HTTP(s) à un hôte cible.

Table de connexion

La table de connexion (sys_connection) est la table de base pour toutes les tables de connexion. Vous pouvez configurer des connexions pour les protocoles suivants :

- Connexion de base pour PowerShell et SSH
- JDBC
- JMS
- HTTP(S)

La table de connexion fait référence à la table d'alias de connexion, qui couple l'alias de connexion aux informations de connexion. Chaque connexion enregistre les informations suivantes :

Propriétés de la connexion de base

Champ	Description
Nom	Nom de la connexion. Ce champ doit être unique dans la table.
Informations d'identification	Spécifiez les informations d'identification à utiliser avec cette connexion. Ceci est facultatif.
Alias de connexion	L'alias de connexion résout votre connexion et vos informations d'identification au moment de l'exécution. Une seule connexion est active par alias de connexion à la fois.
Actif	Cocher pour activer la connexion en cours.
Domaine	Domaine auquel appartient la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les informations d'identification sont uniques pour toutes les connexions actives, si elles ne sont pas vides.

Mise à niveau des informations de connexion

- Les tables de connexion JDBC [jdbc_connection] et de connexion JMS [orch_jms_ds] sont des tables de connexion Orchestration existantes qui s'étendent désormais à partir de la table Connexion [sys_connection]. Les tables s'étendaient à l'origine à partir de sys_metadata. Les données associées au sys_metadata sont supprimées.
- Les tables sont déplacées du module d'extension d'exécution d'Orchestration [com.snc.runbook_automation.runtime] vers le module d'extension Informations d'identification et connexions.
- Le processus de mise à niveau obtient les informations de connexion JDBC et JMS, crée les alias de connexion correspondants et affecte l'alias à sa connexion correspondante.
- Modifications du nom du champ JDBC :
  - Le serveur JDBC est renommé en hôte
  - Le port de la base de données est renommé en port
  - Les données du serveur JDBC et de la base de données migrent vers l'hôte et le port pendant la mise à niveau

Créer une connexion de base pour PowerShell et SSH

Configurez les informations de connexion à utiliser avec une activité ou une action personnalisée qui utilise le protocole PowerShell ou Secure Shell (SSH).

Avant de commencer

Rôle requis : admin ou connection_admin

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Connexions**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **Connexion de base pour PowerShell et SSH.**
4. Renseignez le formulaire.

Champ	Description
Nom	Nom unique de l'enregistrement de connexion.
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Hôte	Nom de domaine complet de l'hôte cible où le système exécute l'activité ou l'action. Par exemple, host.domain.com.
Actif	Sélectionnez cette option pour activer cette connexion.
Domaine	Détermine le domaine dans lequel l'activité s'exécute. Concepteur de flux ne prend pas en charge la séparation de domaine et ignore ce champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Remplacer le port par défaut	Port cible utilisé par la connexion. Si vous laissez ce champ vide, le système utilise la valeur de port par défaut.
Utiliser Serveur MID	Sélectionnez cette option pour vous connecter à l'hôte cible via un Serveur MID fichier . Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID. **Remarque :** PowerShell nécessite un Serveur MID fichier .
Sélection de MID	Option permettant de sélectionner un serveur MID ou une grappe MID spécifique. Choisissez l'une des options suivantes. ○ **Sélection automatique du serveur MID** : votre ServiceNow instance sélectionne le sans entrée manuelle Serveur MID . ○ **Serveur MID spécifique** : votre ServiceNow instance utilise que Serveur MID vous spécifiez. ○ **Grappe MID spécifique** : votre ServiceNow instance utilise la grappe MID que vous spécifiez. Une grappe MID est un groupe de serveurs MID qui permet à votre ServiceNow instance de gérer plusieurs intégrations et d'améliorer la vitesse d'intégration. Pour plus d'informations, consultez Configure a MID Server cluster . Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Centre d'intégration connexion est référencé, et non un enregistrement de Orchestration connexion.
Options	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celles qui Serveur MID sont sélectionnées lors de l'exécution. Pour en savoir plus sur la façon dont a Serveur MID est sélectionné pendant l'exécution, voir Sélection du serveur MID . Ce champ n'est visible que lorsque l'option **Sélectionner automatiquement Serveur MID** est sélectionnée dans la liste Sélection MID.
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste de sélection MID.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée et qu'une **grappe MID spécifique** est sélectionnée dans la liste de sélection MID.

5. Cliquez sur **Envoyer**.

Créer une connexion HTTP(s)

La connexion HTTP(s) fournit les informations que les actions ou activités HTTP(S) personnalisées utilisent pour se connecter.

Avant de commencer

Rôle requis : connection_admin

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Connexions**, cliquez sur **Nouveau** et sélectionnez **Connexion HTTP(s)**.
2. Ajoutez les informations de connexion suivantes, puis cliquez sur **Soumettre** :

Champ	Description
Nom	Nom unique de cette connexion HTTP(s).
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Générateur d'URL	Entrez manuellement l'URL de connexion ou utilisez le système pour créer l'URL en fonction des entrées. Il n'est pas coché par défaut. Si cette option est cochée, l'URL de connexion est calculée à partir des champs suivants : ○ Authentification réciproque : cochez la case si l'authentification réciproque est utilisée. ○ Protocole : si l'authentification réciproque n'est pas utilisée, entrez protocole. La valeur par défaut est HTTPs. ○ Profil du protocole : si l'authentification réciproque est utilisée, entrez le profil du protocole à partir de sys_protocol_profile. ○ Hôte ○ Port ○ Chemin de base : chemin d'accès de la chaîne de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si l'authentification réciproque est cochée, l'URL de connexion est générée : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : Profil du protocole + :// + hôte :port +URL
URL de connexion	Si l'option Générateur d'URL est décochée, entrez l'URL de connexion dans ce champ. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est générée : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : Profil du protocole + :// + hôte :port +URL
Actif	Cochez la case pour activer cette connexion.
Domaine	Déterminez le domaine dans lequel l'action ou l'activité s'exécute.
Utiliser un serveur MID	Activez cette option pour utiliser un Serveur MID pour cette action ou activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Option permettant de sélectionner un serveur MID ou une grappe MID spécifique. Choisissez l'une des options suivantes. ○ **Sélection automatique du serveur MID** : votre ServiceNow instance sélectionne le sans entrée manuelle Serveur MID . ○ **Serveur MID spécifique** : votre ServiceNow instance utilise que Serveur MID vous spécifiez. ○ **Grappe MID spécifique** : votre ServiceNow instance utilise la grappe MID que vous spécifiez. Une grappe MID est un groupe de serveurs MID qui permet à votre ServiceNow instance de gérer plusieurs intégrations et d'améliorer la vitesse d'intégration. Pour plus d'informations, consultez Configure a MID Server cluster . Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Centre d'intégration connexion est référencé, et non un enregistrement de Orchestration connexion.
Options	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celles qui Serveur MID sont sélectionnées lors de l'exécution. Pour en savoir plus sur la façon dont a Serveur MID est sélectionné pendant l'exécution, voir Sélection du serveur MID . Ce champ n'est visible que lorsque l'option

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Sélectionner automatiquement Serveur MID est sélectionnée dans la liste Sélection MID.
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste de sélection MID.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée et qu'une **grappe MID spécifique** est sélectionnée dans la liste de sélection MID.
Délai de connexion	Nombre de millisecondes pendant lesquelles le système attend une connexion de l'hôte réussie. Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Laissez ce champ vide pour utiliser la valeur de délai de connexion par défaut du système. **Remarque :** Évitez de définir la valeur **du délai de connexion** sur zéro, car cela pourrait entraîner l'obsolescence de la connexion.
additional_http_headers (onglet Attributs)	Incluez tous les en-têtes supplémentaires requis, tels que sap-client=100. Si vous ajoutez plusieurs en-têtes, séparez-les par un point-virgule.
odata_ping_url (onglet Attributs)	L'URL ping OData par défaut est /sap/bc/ping. Pour modifier l'URL Ping pour la pulsation OData, sélectionnez l'icône de verrouillage, modifiez l'URL et sélectionnez à nouveau l'icône de verrou.

3. Cliquez sur **Envoyer**.
   Vous pouvez créer une action ou une activité HTTP(s) personnalisée.

Créer une connexion JDBC

La connexion JDBC fournit les informations que les actions ou activités JDBC personnalisées utilisent pour se connecter à diverses bases de données cibles.

Avant de commencer

Vous devez disposer d'un fichier JAR approprié, qu'il soit fourni avec l'instance ou un fichier JAR personnalisé.

Remarque :
L'instance ServiceNow fournit des fichiers mysql-connector-java-5.1.21.jar, sql-server-jdbc-4.0.jar et ojdbc6.jar dans le cadre de la version actuelle, qui prend en charge les bases de données MySQL, SQL Server et Oracle. D'autres bases de données, telles que Sybase ou DB2 Universal, doivent utiliser un fichier JAR personnalisé qui doit être téléchargé sur l'instance avant de définir la connexion JDBC.

Rôle requis : connection_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les informations d'identification JDBC sont récupérées séparément par le modèle du concepteur d'activité et prennent en charge le stockage des informations d'identification externes, telles que CyberArk.

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Connexions**, cliquez sur **Nouveau** et sélectionnez **Connexion JDBC**.
2. Remplissez le formulaire à l'aide des champs de la table.
   La sélection de base de données dans le champ **Format** détermine les champs disponibles.

Champs de connexion JDBC

Champ	Format de base de données	Description
Nom	Tous	Nom unique de cette connexion JDBC. Par exemple, vous pouvez entrer **JDBC MySQLProd**.
Informations d'identification	Tous	Ajoutez des informations d'identification pour le fournisseur JDBC.
Alias de connexion	Tous	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Délai de requête	Tous	Temps écoulé maximal pendant lequel la requête JDBC est autorisée à s'exécuter sans réponse.
Délai de connexion	Tous	Nombre de secondes pendant lesquelles le système attend avant de fermer une connexion JDBC ou une demande de connexion. Par exemple, si la valeur du délai de connexion est de 10 secondes, le système attend 10 secondes pour que la connexion **aboutisse** . Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Si une connexion réussie se produit, la connexion reste ouverte jusqu'à une période d'inactivité de 10 secondes. Une fois que la connexion a été inactive pendant 10 secondes, la connexion est fermée. **Remarque :** Évitez de définir la valeur **du délai de connexion** sur zéro, car cela pourrait entraîner l'obsolescence de la connexion.
Actif	Tous	Cochez la case pour activer cette connexion.
Domaine	Tous	Domaine pour cette table. Par défaut, la table Connexion JDBC [jdbc_connection] s'exécute dans le domaine **global** .
Format	Tous	Type de base de données pour cette connexion. Par défaut, les choix possibles sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Format de base de données	Description
		○ **MySQL** ○ **Oracle** ○ **SQL Server** ○ **Aucun** Vous pouvez ajouter **Sybase** ou **DB2 Universal** à la liste de choix en téléchargeant le fichier JAR du pilote JDBC approprié sur l'instance. Orchestration reconnaît automatiquement ces pilotes lorsqu'ils sont chargés dans le système et les ajoute à cette liste.
Hôte	Oracle, MySQL, SQL Server	Nom d'hôte ou adresse IP du serveur de base de données.
SID Oracle	Oracle	Identificateur de site de base de données Oracle. La valeur par défaut est **orcl**.
Port Oracle	Oracle	Port utilisé par la base de données Oracle. La valeur par défaut est **1521**.
Nom de base de données	MySQL, SQL Server	Nom de la base de données.
Port	MySQL, SQL Server	Port utilisé par la base de données sélectionnée.
Nom d'instance	SQL Server	Nom d'instance pour le SQL Server sélectionné
URL de connexion	Tous	URL que le Serveur MID utilise pour se connecter à la base de données spécifiée. L'URL est créée automatiquement lorsque vous enregistrez le formulaire et est en lecture seule pour les bases de données par défaut. **Remarque :** Si le format sélectionné n'est pas l'une des bases de données par défaut, vous devez créer manuellement l'URL de connexion afin que le serveur MID sache comment établir la connexion.
Pilote JDBC	Aucun, DB2 Universal, Sybase	Pilote JDBC à utiliser pour cette connexion lorsqu'il ne s'agit pas d'une base de données par défaut. **Remarque :** Si vous ajoutez une base de données Sybase ou DB2 Universal, vous devez entrer le nom du pilote dans ce champ et télécharger le fichier JAR du pilote sur l'instance.
Utiliser un serveur MID	Tous	Cocher pour utiliser un Serveur MID pour cette action ou activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Tous	Option permettant de sélectionner un serveur MID ou une grappe MID spécifique. Choisissez l'une des options suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Format de base de données	Description
		○ **Sélection automatique du serveur MID** : votre ServiceNow instance sélectionne le sans entrée manuelle Serveur MID . ○ **Serveur MID spécifique** : votre ServiceNow instance utilise que Serveur MID vous spécifiez. ○ **Grappe MID spécifique** : votre ServiceNow instance utilise la grappe MID que vous spécifiez. Une grappe MID est un groupe de serveurs MID qui permet à votre ServiceNow instance de gérer plusieurs intégrations et d'améliorer la vitesse d'intégration. Pour plus d'informations, consultez Configure a MID Server cluster . Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Centre d'intégration connexion est référencé, et non un enregistrement de Orchestration connexion.
Options	Tous	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celles qui Serveur MID sont sélectionnées lors de l'exécution. Pour en savoir plus sur la façon dont a Serveur MID est sélectionné pendant l'exécution, voir Sélection du serveur MID . Ce champ n'est visible que lorsque l'option **Sélectionner automatiquement Serveur MID** est sélectionnée dans la liste Sélection MID.
Application MID	Tous	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Serveur MID	Tous	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste de sélection MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Format de base de données	Description
Grappe MID	Tous	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée et qu'une **grappe MID spécifique** est sélectionnée dans la liste de sélection MID.

3. Cliquez sur **Envoyer**.

Information associée

Informations d'identification JDBC

Créer une connexion JMS

Configurez votre système pour utiliser Java Messaging Service (JMS) avec une activité ou une action JMS personnalisée.

Avant de commencer

Rôle requis : connection_admin

Pourquoi et quand exécuter cette tâche

Le serveur MID doit disposer des instanciateurs de connexions JMS appropriés pour votre organisation. Configurez ces valeurs dans la `mid.property.jms.command.allowed_factory_names` propriété, qui se trouvent dans **Serveur MID** > **Propriétés**. Les valeurs par défaut de cette propriété peuvent être remplacées par n'importe quelle valeur ou liste de valeurs séparées par des virgules que le fournisseur JMS tiers annonce.

Procédure

1. Accédez à la **Informations d'identification et connexions** > **Connexions**.
2. Cliquez sur **Nouveau**, sélectionnez **Connexion JMS**, remplissez le formulaire, puis cliquez sur **Soumettre**.

Option	Description
Nom	Nom unique de cette fabrique de connexions.
Informations d'identification	Ajoutez des informations d'identification pour le fournisseur JMS.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Instanciateur de contexte initial	Nom de la classe JNDI utilisée pour créer InitialContext. **Remarque :** Par exemple, pour vous connecter à ActiveMQ V5.10 (fournisseur JMS), la valeur est org.apache.activemq.jndi.ActiveMQInitialContextFactory.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
URL du fournisseur	Emplacement de l'installation du fournisseur JMS en cours d'exécution. **Remarque :** Par exemple, pour vous connecter à ActiveMQ V5.1 : tcp://ipAddressOrHost–Name:61616.
Actif	Cochez la case pour activer cette connexion.
Domaine	Déterminez le domaine dans lequel l'action ou l'activité s'exécute.
Utiliser un serveur MID	Activez cette option pour utiliser un Serveur MID pour cette action ou activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Option permettant de sélectionner un serveur MID ou une grappe MID spécifique. Choisissez l'une des options suivantes. ○ **Sélection automatique du serveur MID** : votre ServiceNow instance sélectionne le sans entrée manuelle Serveur MID . ○ **Serveur MID spécifique** : votre ServiceNow instance utilise que Serveur MID vous spécifiez. ○ **Grappe MID spécifique** : votre ServiceNow instance utilise la grappe MID que vous spécifiez. Une grappe MID est un groupe de serveurs MID qui permet à votre ServiceNow instance de gérer plusieurs intégrations et d'améliorer la vitesse d'intégration. Pour plus d'informations, consultez Configure a MID Server cluster . Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser Serveur MID** est cochée et qu'une **grappe MID spécifique** est sélectionnée dans la liste de sélection MID.
Options	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .

3. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.
4. Cliquez sur **Nouveau**, sélectionnez **Informations d'identification JMS**, puis fournissez le nom d'utilisateur et le mot de passe que le MID doit utiliser pour communiquer avec le fournisseur JMS.
   Pour plus d'informations, consultez Informations d'identification JMS.
5. Cliquez sur **Envoyer**.
   Vous pouvez créer une action ou une activité JMS personnalisée.

Créer des attributs de connexion pour Centre d'intégration

Définissez des variables spécifiques à la connexion que vous pouvez utiliser dans les étapes d'intégration Centre d'intégration.

Avant de commencer

Rôle requis :

- Le rôle administrateur est requis pour créer des attributs de connexion.
- Le rôle connection_admin ou administrateur est requis pour affecter les valeurs d'attribut.
- Le rôle action_designer ou administrateur est requis pour utiliser des attributs dans une action personnalisée.

Les attributs de connexion ne sont utilisés que par les étapes d'intégration, qui nécessitent un abonnement à Centre d'intégration. Pour en savoir plus sur l'activation Centre d'intégration, reportez-vous à la section Demander un Centre d'intégration module d'extension .

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez une étape d'intégration, vous devez établir une connexion avec un système externe. Utilisez un alias de connexion et d'informations d'identification au lieu de définir l'inline de la connexion. Un alias vous permet de mettre à jour les détails de la connexion une seule fois, sans avoir à reconfigurer chaque action. Toute étape d'action qui utilise un alias hérite des attributs qui lui sont associés. Studio de workflow affiche les attributs en tant que pastilles de données que vous pouvez faire glisser dans votre étape d'action. Par exemple, vous pouvez créer un attribut de taille de page qui devient un paramètre de requête d'étape REST.

Pour plus d'informations sur la création d'actions personnalisées Studio de workflow , voir Studio de workflow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Alias de connexion et d'informations d'identification**.
2. Créez ou sélectionnez un enregistrement d’alias.
3. Dans la liste connexe Attributs de connexion, cliquez sur **Nouveau**.
4. Définissez l’étiquette d’attribut et le type de champ.
   Pour obtenir la liste des types de champs, consultez Types de champs .
5. Cliquez sur le lien connexe de la vue avancée pour définir les préférences de dictionnaire avancées pour l’attribut.
   Par exemple, pour créer un attribut avec une valeur calculée dynamiquement. Consultez Dictionary entry form .
6. Cliquez sur **Envoyer**.
7. Définissez les valeurs d’attribut dans l’enregistrement de connexion.
   a. Accédez à la **Informations d'identification et connexions** > **Connexions**.
   b. Créez ou sélectionnez un enregistrement de connexion avec le même type de connexion que l’alias.
   c. Dans **Alias de connexion**, sélectionnez l’alias avec les attributs de connexion.
   d. Enregistrez l'enregistrement.
      L’onglet Attributs se remplit avec les attributs de connexion définis dans l’enregistrement d’alias.
   e. Définissez des valeurs pour les attributs.
      Si la **prise en charge de plusieurs connexions actives** est activée pour l’alias, vous pouvez associer plusieurs enregistrements de connexion à un alias et définir des valeurs d’attributs dans chaque enregistrement de connexion. S’il existe plusieurs enregistrements de connexion avec des valeurs d’attribut pour le même alias, la connexion utilisée lorsque le flux s'exécute détermine les valeurs d'attribut. Par exemple, vous activez une action qui utilise un alias avec deux points de terminaison de connexion actifs : production et test. L'attribut se résout à la valeur définie par la connexion utilisée lors de l'exécution.
8. Ajouter l’alias à une étape d’intégration dans Studio de workflow.
   a. Accédez à l’action Studio de workflow et créez-la ou sélectionnez-la.
   b. Ajoutez une étape d’intégration à l’action.
   c. Sous Détails de connexion, ajoutez l’alias pour lequel vous avez créé des attributs.

   Les attributs de connexion associés à l’alias s’affichent sous forme de pastilles de données dans le volet Données.

Remarque :
Le système ne suit pas les changements apportés aux étiquettes d’attributs de connexion et aux types de données après que vous avez associé l’alias à une étape. Pour actualiser l’étiquette d’attribut de connexion ou le type de données, supprimez l’alias de l’étape et ajoutez-le à nouveau.

Introduction aux informations d’identification

Le Serveur MID utilise les informations d’identification que vous créez dans la table Informations d’identification [discovery_credentials] pour accéder aux ressources de Découverte, Orchestration, Mappage des services et Gestion cloud.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment les MID Servers utilisent les informations d'identification

Par défaut, les serveurs MID Windows utilisent les informations d'identification de connexion du service du serveur MID sur l'ordinateur hôte pour détecter Windows les périphériques sur le réseau. Vous devez configurer les informations d'identification du service Windows MID Server de sorte qu'ils disposent au moins de privilèges d'administrateur local. Pour Linux les UNIX machines et les équipements réseau, le Serveur MID utilise les informations d'identification SSH et SNMP configurées dans l'instance dans **Découverte** > **Informations d'identification**.

Les MID Servers qui Orchestration les utilisent doivent avoir accès aux informations d'identification nécessaires pour exécuter des commandes sur les ordinateurs du réseau, comme spécifié par les activités de workflow . Orchestration peut utiliser les mêmes informations d'identification SSH et SNMP que Découverte, mais dispose de deux informations d'identification supplémentaires conçues pour des activités de workflow spécifiques : Windows (pour les activités PowerShell) et VMware.

Chiffrement et déchiffrement

La plateforme stocke les informations d'identification dans un champ chiffré sur la table Informations d'identification [discovery_credentials]. Une fois saisis, ils ne peuvent pas être visualisés.

Lorsque le MID Server demande des informations d'identification, il ServiceNow AI Platform les déchiffre à l'aide du processus suivant :

1. Les informations d'identification sont déchiffrées sur l'instance avec la clé fixe password2.
2. Les informations d'identification sont à nouveau chiffrées sur l'instance avec la clé publique du Serveur MID.
3. Les informations d'identification sont chiffrées sur l'équilibreur de charge avec SSL.
4. Les informations d'identification sont déchiffrées sur le Serveur MID avec SSL.
5. Les informations d'identification sont déchiffrées sur le serveur MID avec la clé privée du serveur MID.

Remarque :
La plateforme ne dispose pas de clés de chiffrement distinctes pour les instances mutualisées.

Ordre des informations d'identification

Les informations d'identification peuvent se voir attribuer une valeur d'ordre dans le formulaire Informations d'identification, ce qui oblige l'application à essayer toutes les informations d'identification à sa disposition dans une certaine séquence. Si vous ne spécifiez pas de valeur d'ordre, l'application teste les informations d'identification de la table Informations d'identification [discovery_credential] au hasard, jusqu'à ce qu'elle en trouve une qui fonctionne. Par exemple, lorsque :

- Orchestration tente d'exécuter une commande sur un serveur SSH, tel qu'un ordinateur Linux ou UNIX.
- Discovery tente d'interroger un appareil SNMP, tel qu'une imprimante, un routeur ou un onduleur.

Après avoir identifié les informations d'identification d'un appareil et Orchestration, Découverte créez une relation entre les informations d'identification et l'appareil à l'aide de la table Relation d'informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'identification [dscy_credentials_affinity]. Toutes les détections ultérieures ou les activités d'Orchestration tentent de faire correspondre les informations d'identification de cette table à un appareil pour lequel il existe une relation. Si les informations d'identification d'un périphérique changent, Découverte Orchestration réessaie toutes les informations d'identification disponibles jusqu'à ce qu'elles créent une nouvelle relation.

Remarque :
Si Orchestration est Découverte installé, et que l'alias d'informations d'identification est activé, plusieurs relations peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification pour chaque relation et insère les informations d'identification de la relation avec l'ordre le plus bas dans la sonde.

Commander des informations d'identification est utile dans les situations suivantes :

- La table des informations d'identification contient de nombreuses informations d'identification, certaines utilisées plus fréquemment que d'autres. Par exemple, la table contient 150 informations d'identification SSH, dont cinq sont utilisées pour se connecter à 90 % des appareils. Il est recommandé de configurer ces cinq informations d'identification avec des numéros d'ordre bas, ce qui les place en haut de la liste d'exécution. Découverte et Orchestration fonctionnent plus rapidement lorsqu'ils essaient d'abord ces informations d'identification courantes. Après la première connexion réussie, l'utilisateur sait quelles informations d'identification ServiceNow AI Platform utiliser la prochaine fois pour chaque appareil.
- Le ServiceNow AI Platform a une sécurité de connexion agressive. Par exemple, configurez les informations d'identification de base de données avec une valeur d'ordre bas si les serveurs de base de données Solaris du réseau ne fournissent que trois tentatives de connexion infructueuses avant de verrouiller le Serveur MID.

Alias d'identification

Des alias d'informations d'identification sont disponibles pour Découverte et Orchestration.

Les alias pour Découverte permettent à un administrateur d'effectuer les opérations suivantes :

- Appliquez un comportement de filtrage des informations d'identification avec des niveaux de conformité configurables.
- Affectez plusieurs alias d'informations d'identification à une planification de découverte.
- Empêchez la création d'affinités d'identifiants qui utilisent des identifiants inappropriés ou sensibles. Pour en savoir plus, consultez Affinités d'informations d'identification.

Les alias pour Orchestration permettent aux créateurs de workflows d'effectuer les opérations suivantes :

- Affecter des informations d'identification individuelles à n'importe quelle activité dans un workflow Orchestration
- Affecter des informations d'identification individuelles à n'importe quelle action dans Concepteur de flux
- Affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
- Affectez des informations d'identification différentes à chaque occurrence de la même action dans le flux du concepteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Banques d'identifiants externes

Si vous ne souhaitez pas que les informations d'identification soient stockées dans votre instance, vous pouvez utiliser des référentiels d'informations d'identification externes. Les banques d'identifiants externes enregistrent les informations d'identification dans un site externe auquel votre instance peut accéder. CyberArk est la seule banque d'identifiants externes prise en charge. Toutefois, d'autres banques externes peuvent être configurées à l'aide de l'API ServiceNow.

Créer un alias de connexion et d'informations d'identification

Définissez un alias pour étiqueter un enregistrement d'informations d'identification ou de connexion.

Avant de commencer

Rôle requis :

- Le rôle administrateur est requis pour créer un alias.
- Les rôles credential_admin et connection_admin ont un accès en lecture à l'enregistrement d'alias.

Pourquoi et quand exécuter cette tâche

L'alias de connexion et d'informations d'identification définit un alias qui identifie un enregistrement d'informations d'identification ou de connexion. L'alias contient ces champs.

Procédure

1. Accédez à la **Tous** > **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Complétez les champs du formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise de l'enregistrement d'informations d'identification migre vers un alias de connexion et d'informations d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas changé le nom pour respecter les restrictions de nommage.
ID	Identificateur unique pour l'alias de connexions et d'informations d'identification, basé sur le format `scope_name.alias_name`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Si le périmètre est global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ○ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Type	Sélectionnez **Informations d'identification** ou **Connexion et informations d'identification**. La valeur par défaut est Connexion et Informations d'identification.
Application	Périmètre de l'application auquel l'alias de connexion et d'informations d'identification est affecté. Le champ d'application de la session en cours que vous avez sélectionné en dernier dans le sélecteur d'application s'affiche. ○ Par exemple, **Global** s'affiche s'il s'agit du champ d'application actuel de cette session. ○ Vous pouvez modifier le périmètre dans le sélecteur d'application avant de créer un alias. Pour en savoir plus sur les périmètres de l'application et sur la manière de les sélectionner, voir : ▪ Périmètre de l'application ▪ Select an application from the application picker
Type de connexion	Nom du type de connexion, soit De base, HTTP, JDBC, JMS ou Kafka. La valeur par défaut est HTTP.
Prendre en charge plusieurs connexions actives	Désignateur indiquant si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et associez-les à l'alias à l'aide de la liste connexe Connexions.
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez Politique des nouveaux essais .
Modèle de configuration	Modèle de configuration à utiliser pour créer un enregistrement de connexion et d'informations d'identification.

4. Cliquez sur **Enregistrer**.
La liste connexe Connexions et attributs de connexion s'affiche.

Liste connexe	Description
Connexions	Enregistrements de connexion associés à cet alias. Après avoir créé l'alias, vous pouvez définir des enregistrements de connexion et les associer à l'alias. Si **l'option Prendre en charge plusieurs connexions actives** est sélectionnée, vous pouvez associer plusieurs connexions à un alias.
Attributs de connexion	Attributs de la connexion. Définissez des données spécifiques à une connexion et utilisez-les dans une étape d'intégration Centre d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour Centre d'intégration.
Alias enfants	Alias enfants associés à l'alias parent. Après avoir créé un alias de connexion et d'informations d'identification, vous pouvez créer un *alias enfant* pour configurer plusieurs connexions pour la même intégration d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Connexions	Enregistrements de connexion associés à cet alias. Après avoir créé l'alias, vous pouvez définir des enregistrements de connexion et les associer à l'alias. Si **l'option Prendre en charge plusieurs connexions actives** est sélectionnée, vous pouvez associer plusieurs connexions à un alias.
Attributs de connexion	Attributs de la connexion. Définissez des données spécifiques à une connexion et utilisez-les dans une étape d'intégration Centre d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour Centre d'intégration.

5. **Facultatif :** Si vous souhaitez créer un nouvel identifiant et une nouvelle connexion associés à votre alias d'informations d'identification, sous *Related Links*, cliquez sur **Créer une nouvelle connexion et un nouvel identifiant de connexion**.
   Les enregistrements de connexion et d'informations d'identification qui en résultent sont basés sur un modèle de configuration prédéfini. Consultez les modèles de configuration de connexion et d'informations d'identification.
6. **Facultatif :** Si vous souhaitez créer un alias enfant pour votre alias de connexion et d'informations d'identification, dans la liste connexe **Alias enfants** , sélectionnez **Nouveau**.

   a. Donnez un nom à l'alias enfant et sélectionnez **Soumettre**.
      L'alias enfant hérite des propriétés de l'alias parent. Vous pouvez ensuite configurer un alias enfant pour qu'il contienne son propre ensemble d'informations de connexion et d'identification.

Que faire ensuite

Créez un ou plusieurs enregistrements de connexion à associer à l'alias ou aux alias enfants. Pour plus d'informations sur la création de connexions, reportez-vous à la section Mise en route des connexions. Ajoutez des attributs de connexion à l'alias pour mettre les métadonnées de connexion à la disposition des flux Studio de workflow.

Configurer l'intégration OAuth via Serveur MID

Créez un enregistrement de connexion qui permet l'envoi d'une demande de jeton OAuth à un serveur tiers via un Serveur MID.

Avant de commencer

Confirmez que vous êtes abonné au programme d'installation du pack standard de Centre d'intégration ServiceNow. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Rôle requis : admin

Procédure

Configurez la connexion à l'aide d'un modèle de configuration.

a. Accédez à la **Tous** > **Centre d'intégration** > **Modèles de configuration**.

b. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **le type d'accord Connexion HTTP avec Informations d'identification du client OAuth**.

d. Mettez à jour le formulaire, au besoin.
Par exemple, vous pouvez fournir le champ d'application dans les champs `oauth_entity_profile_scope` et `oauth_entity_scope` de la section Modèle de données par défaut. Pour apprendre à créer un modèle de configuration, reportez-vous à la section Créer un modèle de configuration.

e. Sélectionnez **Soumettre**.
Vous avez créé le modèle de configuration.

f. Accédez à la **Tous** > **Centre d'intégration** > **Alias de connexion et d'informations d'identification**.

g. Mettez à jour le formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise de l'enregistrement d'informations d'identification migre vers un alias de connexion et d'informations d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas changé le nom pour respecter les restrictions de nommage.
Application	Identificateur unique pour l'alias de connexions et d'informations d'identification, basé sur le format `scope_name.alias_name`. ○ Si le périmètre est global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ○ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Alias parent	Option permettant de sélectionner l'alias sous lequel vous créez cet alias de connexion et d'informations d'identification. L'alias de connexion et d'informations d'identification que vous créez est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	un alias enfant. Un alias enfant est répertorié sous l'onglet **Alias enfants** sur la page de l'alias de connexion et d'informations d'identification parent. 
Type	Option pour indiquer le type d'alias que vous créez. Choisissez parmi les options suivantes. ○ Informations d'identification : alias qui contient un enregistrement d'informations d'identification. ○ Connexion et informations d'identification : alias qui contient à la fois l'enregistrement de connexion et d'informations d'identification. Cette option est sélectionnée par défaut. Confirmez que la connexion et les informations d'identification sont sélectionnées.
Prendre en charge plusieurs connexions actives	Désignateur indiquant si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et associez-les à l'alias à l'aide de la liste connexe Connexions.
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez Politique des nouveaux essais .
Modèle de configuration	Option permettant de sélectionner le modèle de configuration à partir duquel vous créez l'alias de connexion et d'informations d'identification. Sélectionnez le modèle du type **Connexion HTTP avec type d'accord Informations d'identification du client OAuth** que vous avez créé.

h. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement d'alias de connexion et d'informations d'identification.

i. Accédez à la **Tous** > **Centre d'intégration** > **Tableau de bord des connexions**.

j. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement d'alias de connexion et d'informations d'identification que vous avez créé.

k. Sur l'enregistrement de l'alias de connexion et d'informations d'identification, sélectionnez **Afficher les détails**.

l. Sélectionnez **Configurer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

m. Remplissez le formulaire.

Enregistrement de la connexion

Champ	Description
Nom de la connexion	Nom de l'enregistrement de connexion. Vous ne pouvez pas mettre à jour le nom.
URL de connexion	Option permettant de fournir l'URL qui se connecte au serveur tiers.
Utiliser MID	Option permettant de spécifier que vous souhaitez envoyer des demandes de jetons OAuth via un serveur MID. **Important :** Confirmez que l'option est sélectionnée.
Sélection de MID	Option permettant de spécifier si vous souhaitez utiliser un serveur MID spécifique, activer la sélection automatique de serveur MID ou utiliser une grappe MID. Choisissez une des options suivantes. ○ Sélectionner automatiquement Serveur MID ○ Serveur MID spécifique ○ Grappe MID spécifique
Options	Option permettant de sélectionner une ou plusieurs options de Serveur MID. Les options définissent les fonctions spécifiques d'un serveur MID dans une plage d'adresses IP, ce qui permet à une application de sélectionner le serveur MID le plus approprié. Sélectionnez l'icône des options (+) pour sélectionner une ou plusieurs options. **Remarque :** Cette option s'affiche si vous sélectionnez **Sélectionner automatiquement Serveur MID** dans le champ Sélection MID.
Application MID	Option permettant de spécifier une application MID ou d'accepter le choix d'application par défaut. **Remarque :** Cette option s'affiche si vous sélectionnez **Sélectionner automatiquement Serveur MID** dans le champ Sélection MID. Par défaut, l'option **TOUT** est sélectionnée.
Serveur MID	Option permettant de sélectionner un serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Cette option s'affiche si vous sélectionnez **Serveur MID spécifique** dans le champ Sélection MID.
Grappe MID	Option permettant de sélectionner une grappe MID. **Remarque :** Cette option s'affiche si vous sélectionnez **Grappe MID spécifique** dans le champ Sélection MID.
ID client OAuth	Option permettant de spécifier l'ID client.
Secret client OAuth	Option permettant de spécifier le secret client.
Se connecter au serveur d'authentification via serveur MID	Option permettant de spécifier que la connexion entre l'instance ServiceNow et le serveur d'authentification s'effectue via le serveur MID. **Important :** Confirmez que l'option est sélectionnée.
URL du jeton OAuth	Option permettant de spécifier l'URL du jeton OAuth utilisée pour demander des jetons OAuth.

n. Sélectionnez **Configurer et obtenir le jeton OAuth**.
L'enregistrement de connexion et d'informations d'identification est créé.

Alias d'informations d'identification pour Découverte

Alias d'informations d'identification permettant à Découverte un administrateur d'utiliser des informations d'identification spécifiques sur les calendriers Discovery. Vous pouvez configurer des comportements pour vos alias qui déterminent la rigueur avec laquelle le système applique leur utilisation.

Sans alias d'informations d'identification, les calendriers de découverte peuvent accéder à toutes les informations d'identification définies dans l'instance. Ce comportement peut ne pas être souhaitable dans certaines circonstances, en particulier pour les informations d'identification avec des privilèges élevés. Les alias d'informations d'identification permettent un meilleur contrôle sur les informations d'identification qu'un calendrier de découverte est autorisé à utiliser et empêchent l'exposition inutile des informations d'identification avec des privilèges élevés.

Fonctionnement des alias d'identification

Une règle métier appelée *Insérer des relations de découverte et des alias d'informations d'identification* (précédemment nommée *Insérer une relation de découverte*) s'exécute lorsqu'un enregistrement (une tâche pour effectuer la découverte) est inséré dans la file d'attente ECC.

La règle métier associe les alias d'informations d'identification définis dans le calendrier de découverte à la sonde, de sorte que lorsque la sonde atteint le serveur MID sur le chemin de l'exécution de la découverte, le serveur MID sait exactement quelles informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'identification il peut utiliser pour tenter d'accéder à l'appareil que la sonde a été envoyée pour analyser.

Le MID Server filtre les informations d'identification par relation puis par balises, le cas échéant. Les informations d'identification doivent correspondre à toutes les balises d'informations d'identification. Le serveur MID itère jusqu'à ce qu'il trouve une information d'identification qui fonctionne.

Si la règle métier détermine qu'il existe une relation pour l'appareil, elle identifie les *credential_id* appropriées à utiliser. Il s'agit de *l'sys_id* de l'enregistrement dans la table Informations d'identification [discovery_credentials].

Lorsque la plateforme rencontre une relation avec une valeur d'alias d'informations d'identification, définie comme *credential_alias* dans la règle métier, la règle métier détermine si les informations d'identification référencées par la relation ont ou non l'alias spécifié. Si c'est le cas, la règle métier sélectionne le *credential_id* de l'alias et transmet cette valeur au serveur MID.

Si un alias d'informations d'identification est défini pour un calendrier et que le calendrier est configuré pour utiliser cet alias, le calendrier ignore toute relation d'informations d'identification à cible, *mais uniquement si les informations d'identification elles-mêmes ne sont associées à aucun autre alias d'informations d'identification*. Si l'identifiant n'a pas d'alias d'identifiant de connexion, toutes les autres relations qui existent pour le système cible sont vérifiées.

Créer un alias d'informations d'identification de découverte

Créez l'alias, puis ajoutez-le à des informations d'identification dans l'enregistrement des informations d'identification. Vous pouvez ajouter des informations d'identification à plusieurs alias et ajouter plusieurs informations d'identification à un seul alias.

Avant de commencer

Rôle requis : admin, credential_admin (accès en lecture seule) connection_admin (accès en lecture seule)

Pourquoi et quand exécuter cette tâche

Un calendrier de découverte utilise uniquement les informations d'identification contenues dans les alias définis pour ce calendrier.

Remarque :
Si un alias d'informations d'identification est défini pour un calendrier, il ignorera toute relation d'informations d'identification précédemment existante entre les informations d'identification et la cible détectée dans un calendrier configuré pour utiliser cet alias d'informations d'identification.

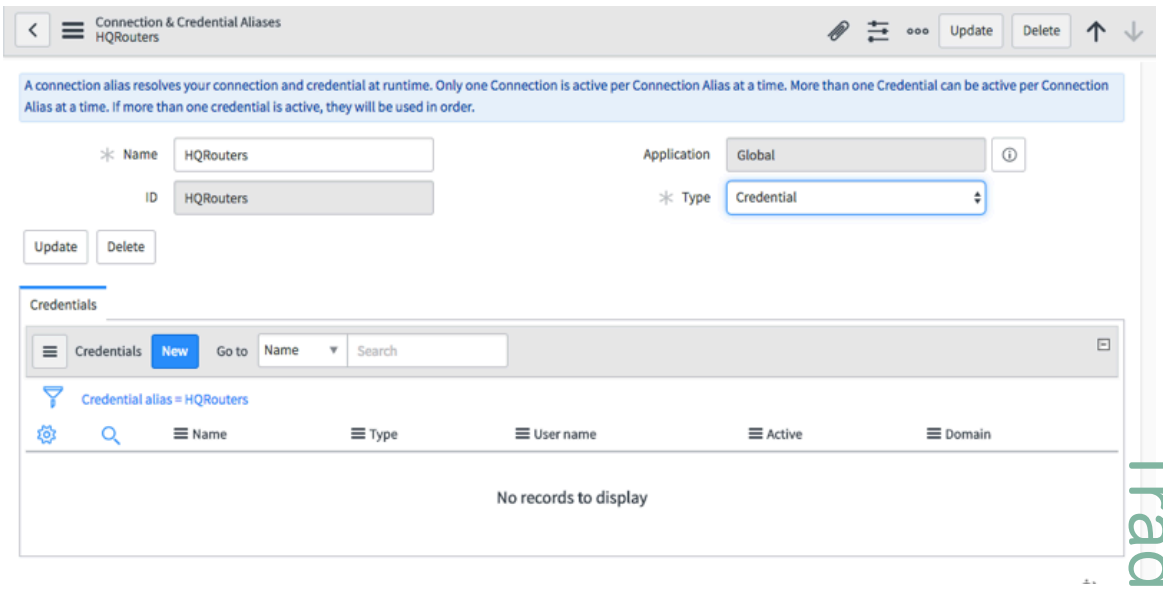
Procédure

1. Créez un alias.
   a. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
   b. Cliquez sur **Nouveau**.
   c. Saisissez un nom unique pour l'alias et sélectionnez **Informations d'identification** pour le **type d'alias**.
   d. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste connexe **Informations d'identification** s'affiche. Vous pouvez ajouter de nouvelles informations d'identification pour cet alias dans cette liste, mais pas les informations d'identification existantes.

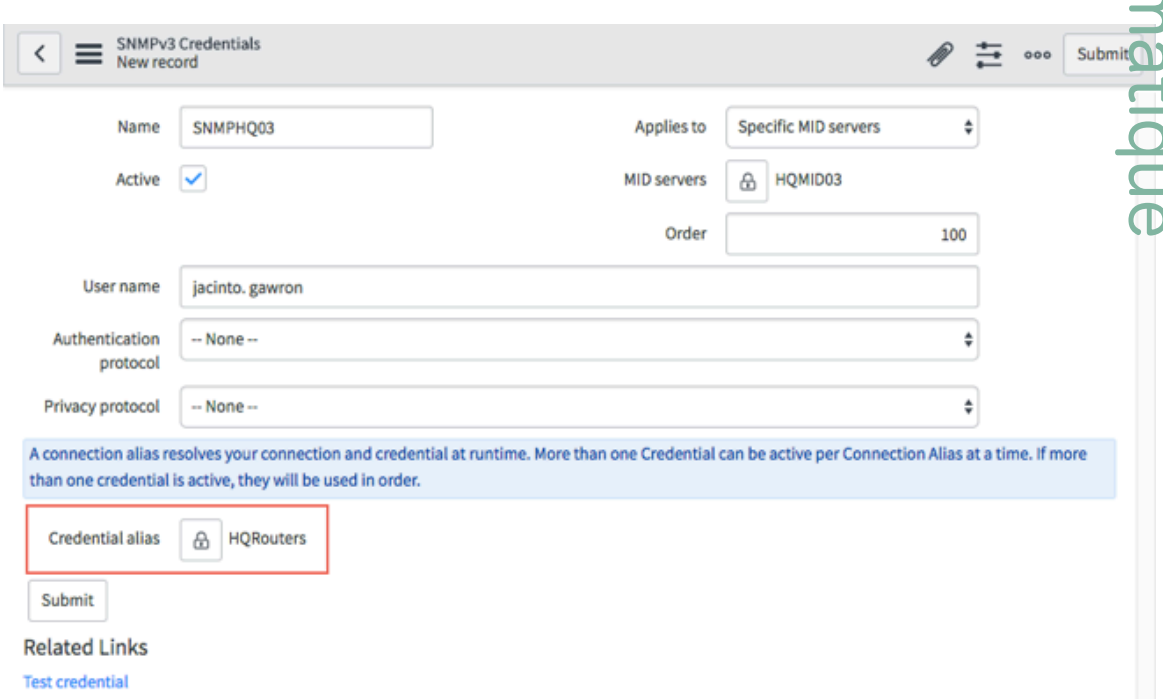


2. Configurez les informations d'identification pour le nouvel alias.

a. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.

b. Sélectionnez les informations d'identification existantes dans la liste ou cliquez sur **Nouveau** pour créer des informations d'identification.

c. Dans l'enregistrement des informations d'identification, déverrouillez le champ **Alias d'informations d'identification** et sélectionnez l'alias que vous avez créé.

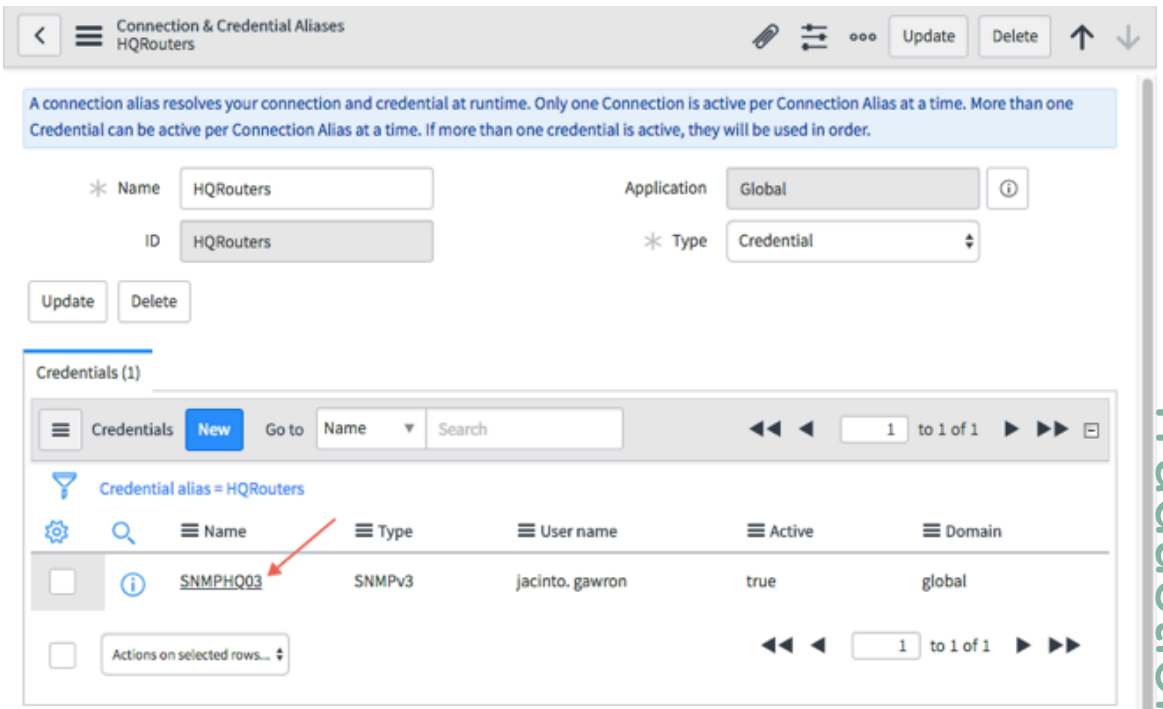


d. Enregistrez ou soumettez l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Retourner à **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification** et ouvrez votre nouvel alias.
   Les informations d'identification que vous avez jointes à l'alias apparaissent maintenant dans la liste connexe.



4. Pour créer des informations d'identification supplémentaires pour cet alias, cliquez sur **Nouveau** dans la liste connexe et sélectionnez un type d'informations d'identification.
   Le nom de l'alias est pré-renseigné dans le champ **Alias d'informations d'identification** de l'enregistrement d'informations d'identification.
5. Renseignez les champs dans le formulaire et envoyez l'enregistrement.

Alias d'informations d'identification pour les activités Orchestration

L'alias d'informations d'identification donne à un administrateur plus de contrôle sur les informations d'identification utilisées dans les activités Orchestration.

Cela est utile lorsqu'une activité nécessite des informations d'identification spécifiques pour effectuer une tâche. Vous pouvez utiliser une balise d'informations d'identification pour affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affecter des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.

L'alias d'informations d'identification interagit avec la relation d'informations d'identification pour déterminer quelles informations d'identification doivent être utilisées pour une activité Orchestration.

Fonctionnement de l'alias d'informations d'identification

Une règle métier appelée *Insérer une relation de découverte* (renommée à partir de Insérer une relation d'informations d'identification dans la version Geneva) s'exécute lorsqu'un enregistrement est inséré dans la file d'attente ECC. Cette règle détermine s'il existe une relation d'informations d'identification pour l'appareil et identifie la *credential_id* appropriée (le *sys_id* de l'enregistrement dans la table Informations d'identification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[discovery_credentials]) à utiliser. Lorsque la plateforme rencontre une relation avec une valeur d'alias d'informations d'identification définie (*credential_alias* dans la règle métier), la règle métier détermine si les informations d'identification référencées par la relation ont l'alias spécifié. Si c'est le cas, la règle métier sélectionne *l'credential_id* de l'alias d'informations d'identification et transmet cette valeur au serveur MID. Si les informations d'identification ne possèdent pas l'alias d'informations d'identification spécifié, toutes les autres relations existantes pour le système cible sont vérifiées. Si aucune relation ne fait référence à des informations d'identification balisées de manière appropriée, le serveur MID itère la table Informations d'identification *[discovery_credentials]* et sélectionne l'information d'identification avec la balise appropriée. Le Serveur MID crée ensuite une nouvelle relation pour ces informations d'identification.

Créer et tester vos informations d'identification

Créez et testez les informations d'identification requises par Découverte, Mappage des services, Cloud Management et Orchestration pour accéder au matériel et aux logiciels de votre réseau.

Avant de commencer

Rôle requis : admin

Passez en revue votre politique de sécurité et vos options avec l'équipe de sécurité de votre organisation.

Pourquoi et quand exécuter cette tâche

Cette tâche contient des procédures générales pour la création des informations d'identification. Consultez la documentation relative à votre type d'informations d'identification pour plus de détails sur les champs et exigences spécifiques.

Types d'informations d'identification pris en charge

Informations d'identification applicatives	Informations d'identification d'authentification de base	Informations d'identification de serveur Chef
Informations d'identification CIM	Informations d'identification dans le cloud	Informations d'identification du référentiel d'images de conteneurs
Informations d'identification Infoblox	Informations d'identification JDBC	Informations d'identification JMS
Informations d'identification OAuth 2.0	Informations d'identification SAP	Informations d'identification SNMP
Informations d'identification SSH	Informations d'identification VMware	Informations d'identification Windows

Remarque :
Pour améliorer la sécurité, limitez le champ d'application des informations d'identification à un Serveur MID ou à un calendrier spécifique afin d'éviter les informations d'identification inutiles.

Procédure

1. Accédez à l'un de ces modules :
   - **Découverte** > **Informations d'identification**
   - **Mappage des services** > **Informations d'identification**
   - **Orchestration** > **Informations d'identification**
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sur la page Informations d'identification, cliquez sur un lien pour le type d'informations d'identification et remplissez le formulaire.

   Consultez la documentation pour connaître le type d'information d'identification que vous avez sélectionné pour plus d'informations.

   Vous pouvez d'abord soumettre un enregistrement d'informations d'identification, puis le tester ultérieurement, ou tester les informations d'identification immédiatement avant de l'enregistrer.

   Le test des informations d'identification est pris en charge pour ces types d'informations d'identification :

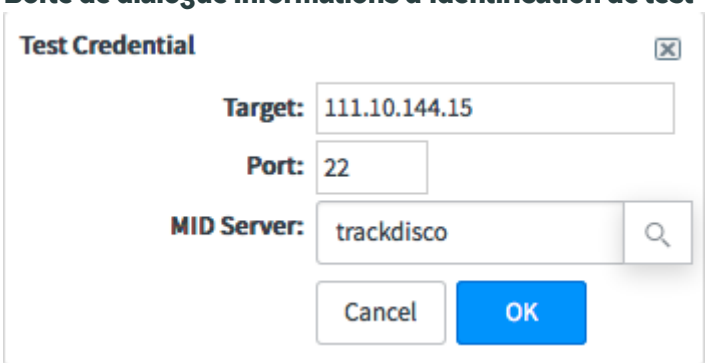
   - Clés privées SSH
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS

4. Sous **Liens connexes**, cliquez sur **Tester les informations d'identification**.

   Remarque :
   Les informations d'identification sont chiffrées à tout moment pendant le test.

5. Renseignez les champs de la boîte de dialogue Tester les informations d'identification.

Boîte de dialogue Informations d'identification de test



Champs de test des informations d'identification

Champ	Description	Type d'informations d'identification
Cible	Hôte cible sur lequel ces informations d'identification sont exécutées. Cette valeur doit être une adresse IP pour tous les types d'informations d'identification, à l'exception de VMware, qui peut être l'URL de l'hôte. Vous ne pouvez cibler aucun MID Server.	Tous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description	Type d'informations d'identification
	Remarque : Pour JMS, il s'agit de l'URL du fournisseur. Les informations contenues dans cette URL indiquent à JNDI comment trouver le fournisseur JMS et y accéder. Un exemple de valeur pour la connexion à ActiveMQ V5.1 est `tcp://ipAddressOrHostName:61616`.	
Port	Port sur la cible à utiliser pour ce test. Le système préremplit ce champ avec le port par défaut pour le type d'information d'identification sélectionné.	Tous
Serveur MID	Serveur MID à utiliser pour ce test. Vous devez utiliser un Serveur MID Windows pour tester les informations d'identification Windows. Seuls les MID Servers **En service** et **Validés** sont disponibles.	Tous
Type de base de données	Type de base de données sur laquelle tester ces informations d'identification.	JDBC
Adresse de la carte	Nom de la base de données sur laquelle tester ces informations d'identification.	JDBC
Instanciateur de contexte initial	Nom de la classe JNDI utilisée pour créer InitialContext. À l'aide de cette **fabrique de contexte initial**, divers objets JMS, tels que la connexion JMS, sont créés. Par exemple, pour vous connecter à ActiveMQ V5.10, (fournisseur JMS), la valeur de ce champ sera `org.apache.activemq.jndi.ActiveMQInitialContextFactory`	JMS

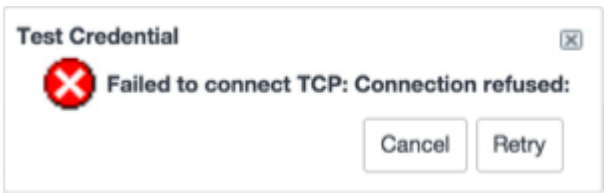
6. Cliquez sur **OK** pour commencer le test.
   Un indicateur s'affiche, montrant que le système tente de contacter la cible à l'aide des informations d'identification que vous avez fournies. Lorsque l'instance se connecte à la cible, elle affiche un message de réussite. Si l'instance rencontre un problème avec les entrées de test que vous avez fournies, elle affiche le message d'erreur approprié. Voici quelques messages d'erreur courants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

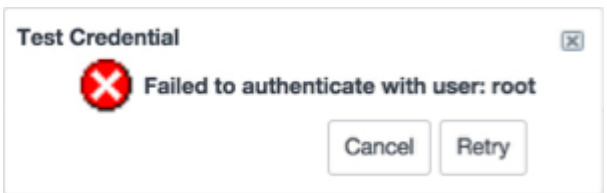
- Cible ou numéro de port incorrect :

  Échec de la connexion TCP

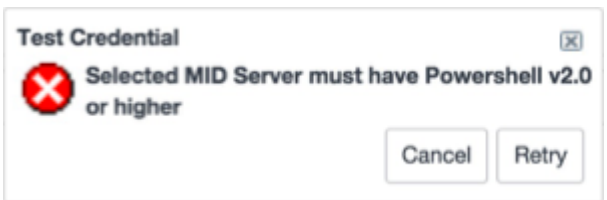
- Nom d'utilisateur ou mot de passe incorrect :

  Échec de l'authentification

- Informations d'identification de Serveur MID pour Windows incorrectes :

  Erreur de Serveur MID

7. Cliquez sur **Réessayer** pour ouvrir la boîte de dialogue tester les informations d'identification et corriger l'erreur d'entrée.
8. Lorsque votre test d'informations d'identification est réussi, cliquez sur **Envoyer** pour sauvegarder l'enregistrement.

> **Important :**
> Le test des informations d'identification ne garantit pas que les informations d'identification disposent des privilèges nécessaires pour les tâches de workflow Découverte ou Orchestration prévues.

Informations d'identification de la tour Ansible

Les informations d'identification Ansible Tower sont nécessaires pour accéder à votre compte de gestion des configurations Ansible. Utilisez ces informations d'identification pour gérer les ressources Ansible via l'application Gestion cloud .

Pour intégrer Cloud Provisioning and Governance avec le compte de gestion des configurations Ansible, vous devez configurer le nom d'utilisateur et le mot de passe du compte administrateur dans Ansible.

Champs de formulaire pour les informations d'identification de la tour Ansible

Champ	Description
Nom	Fournissez un nom descriptif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire pour les informations d'identification de la tour Ansible (suite)

Champ	Description
Nom d'utilisateur/ mot de passe	Entrez les informations d'identification d'authentification pour l'utilisateur de la tour Ansible avec les droits d'administrateur.

Remarque :
Vous n'avez pas besoin de configurer les autres champs.

Informations d'identification de clé API

Une clé API est un code unique transmis à une API pour identifier l'application ou l'utilisateur appelant.

Informations d'identification de clé API

Champs de formulaire Informations d'identification de clé API

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Clé API	Entrez la clé API.
Alias d'identification	Autorisez les créateurs de flux et de workflow à affecter des informations d'identification individuelles à n'importe quelle activité d'un flux ou d'un workflow, ou à affecter des informations d'identification différentes à chaque occurrence du même type d'activité dans un flux ou un workflow.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification applicatives

Certaines applications nécessitent des informations d'identification en plus des informations d'identification requises par l'ordinateur hôte. Les informations d'identification requises pour accéder à ces applications sont appelées informations d'identification applicatives.

Les informations d'identification classiques contiennent un nom d'utilisateur et un mot de passe permettant de se connecter à un appareil ou à une application. Bien que la plupart des applications n'aient besoin que d'un seul identifiant pour se connecter, les hôtes et les applications disposent parfois d'informations d'identification distinctes pour plus de sécurité. Par exemple, ABAP SAP Central Services (ASCS) nécessite des informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'identification applicatives en plus des informations d'identification de l'hôte SSH ou Windows pour le serveur qui héberge ASCS.

Remarque :
ServiceNow les applications font référence aux appareils et aux applications qui composent une instance de service en tant qu'éléments de configuration (CI).

Comme pour les informations d'identification d'hôte, vous affectez des informations d'identification applicatives à Serveurs MID.

Vous créez des informations d'identification applicatives par type de CI. Par exemple, le type de CI pour ASCS est SAP ASCS Application [cmdb_ci_appl_sap_ascs]. Le modèle préconfiguré pour la détection des CI appartenant à ce type de CI contient des commandes qui nécessitent qu'un Serveur MID utilise les informations d'identification applicatives pour ce type de CI. S'il y a plusieurs informations d'identification configurées pour ce type de CI, l'équipe Serveur MID essaie d'utiliser ces informations d'identification dans l'ordre que vous définissez jusqu'à ce qu'il trouve les informations d'identification qui conviennent.

Vérifiez les informations sur les besoins Découverte dans la documentation ServiceNow afin de déterminer si vous devez configurer des informations d'identification applicatives pour des CI d'application spécifiques. Il n'est pas nécessaire de configurer les informations d'identification applicatives si Découverte les prérequis ne le mentionnent pas.

Champs du formulaire Informations d'identification applicatives

Champ	Description
Nom	Nom des informations d'identification. Utilisez un nom descriptif comme « Base de données Oracle » ou « Base de données Oracle London » (pour une base de données Oracle). N'utilisez pas d'espaces ou de caractères spéciaux pour le nom des informations d'identification.
Actifs	Cochez la case pour utiliser les informations d'identification.
Nom d'utilisateur	Entrez le nom d'utilisateur réel des informations d'identification applicatives.
Mot de passe	Entrez le mot de passe réel des informations d'identification applicatives. N'utilisez pas d'espaces ou de caractères spéciaux pour le nom des informations d'identification.
Type de CI	Sélectionnez un type de CI auquel le CI appartient.
Alias d'informations d'identification	Créez un alias pour affecter des informations d'identification spécifiques à des calendriers de détection spécifiques. Lorsque vous affectez un alias, vous devez identifier le nom de table du type de CI dont les informations d'identification applicatives sont utilisées par l'application. Les applications peuvent utiliser des informations d'identification applicatives d'un type de CI différent du leur. Pour une application spécifique, consultez la liste de la table appropriée : • SAP ABAP Central Services (ASCS) : cmdb_ci_appl_sap_ascs • IBM Security Access Manager appliance : cmdb_ci_app_server_webseal • Instance SAP Central : cmdb_ci_appl_sap_ascs • SAP Central Services (SCS) : cmdb_ci_appl_sap_ascs • Evaluated Receipt Settlement (ERS) SAP : cmdb_ci_appl_sap_ascs • Grappe Java SAP : cmdb_ci_appl_sap_ascs • Instance de boîte de dialogue SAP NetWeaver : cmdb_ci_appl_sap_ascs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du formulaire Informations d'identification applicatives (suite)

Champ	Description
	• Messagerie Microsoft Exchange (pour Microsoft Exchange) : cmdb_ci_exchange_mailbox • Base de données SQL Microsoft : cmdb_ci_db_mssql_instance • Serveur MySQL : cmdb_ci_db_mysql_instance • File d'attente avancée Oracle : cmdb_ci_db_ora_instance • Oracle Database : cmdb_ci_db_ora_instance • Oracle E-Business Suite : cmdb_ci_db_ora_instance • Module Oracle WebLogic : cmdb_ci_app_server_weblogic • TIBCO Enterprise Message Service (EMS) : cmdb_ci_appl_tibco_message
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification d'authentification de base

Le type d'informations d'identification d'authentification de base gère l'accès au stockage des informations d'identification d'authentification de base.

Ces champs sont disponibles dans le formulaire Informations d'identification pour l'authentification de base.

Formulaire Informations d'identification pour l'authentification de base

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **Authentification de base**.
Nom d'utilisateur	Entrez le nom d'utilisateur.
Mot de passe	Entrez le mot de passe.
ID de certification	Saisissez la clé unique configurée pour ces informations d'identification dans le système de stockage des informations d'identification externe CyberArk . L'ID d'informations d'identification peut être utilisé comme remplacement sécurisé lorsque plusieurs coffres-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification pour l'authentification de base (suite)

Champ	Valeur d'entrée
	forts sont utilisés. Par défaut, la syntaxe du champ **ID d'informations d'identification** est la suivante : `<safe name>:<Credential ID>`. Si le nom Safe est omis, un nom Safe doit être défini dans le fichier config.xml . Pour remplacer le caractère du caractère de séparation par défaut par un autre caractère, remplacez la valeur par le paramètre facultatif `ext.cred.safe_name` . Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Stockage externe** est cochée.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification de serveur Chef

Les informations d'identification du serveur Chef permettent d'accéder aux intégrations Chef avec l'instance.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type serveur Chef. Ces informations proviennent des paramètres que vous avez configurés lors de l'installation du serveur Chef .

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom de l'administrateur	Fournissez le nom d'administrateur que vous avez créé lors de l'installation du serveur Chef.
Clé d'administrateur	Entrez la clé privée RSA générée par le serveur Chef lors de la création de l'administrateur.
Nom de validateur	Saisissez le validateur.
Clé de validateur	Entrez la clé privée RSA générée par le serveur Chef lorsque vous avez créé une organisation.
Nom du certificat	Entrez le nom de la certification.
Clé du certificat	Entrez la clé de certification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification CIM

Le type d'informations d'identification CIM gère l'accès à un serveur CIM (également appelé CIMOM pour « Common Information Model Object Manager ») afin d'obtenir des informations sur les serveurs ESX VMware. Ce type d'informations d'identification est disponible pour Découverte.

Ces champs sont disponibles dans le formulaire Informations d'identification pour CIM.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Configurer les périphériques de stockage NetApp pour les informations d'identification CIM

Les périphériques de stockage NetApp nécessitent une configuration supplémentaire pour Découverte les explorer.

Avant de commencer

Rôle requis : admin

Procédure

1. Installez l'agent SMI-S sur l'hôte de l'appareil de stockage.

   Consultez le Guide d'installation et de configuration de Data ONTAP SMI-S Agent 5.2 pour connaître les instructions et les exigences.

   Remarque :

   ServiceNow ne maintient pas la documentation sur ce site. Ce document peut être modifié sans préavis.

2. Créez un compte utilisateur et un mot de passe pour l'agent SMI-S.
3. Créez un enregistrement d'informations d'identification pour les informations d'identification de l'agent SMI-S.
   Définissez le type d'informations d'identification **sur CIM**.

Informations d'identification dans le cloud

Les types d'informations d'identification cloud gèrent l'accès aux applications basées sur le cloud, y compris Amazon Web Services et le cloud Microsoft Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles AWS Identity and Access Management (IAM)

Si un serveur MID est installé sur Amazon EC2 dans un cloud AWS, et que ce serveur MID est configuré pour détecter des ressources dans le cloud, vous pouvez utiliser les informations d'identification de sécurité fournies par les rôles AWS Identity and Access Management (IAM) plutôt que les informations d'identification gérées sur votre instance. Ces informations d'identification AWS accordent des autorisations dans le cloud via un *profil d'instance*, en fonction des rôles. Ces informations d'identification sont temporaires et tournent automatiquement selon un intervalle configurable. Lorsqu'un rôle IAM est défini sur le serveur MID. Pour plus d'informations, consultez Configurer le serveur MID pour les rôles AWS IAM .

La Découverte ignore les informations d'identification stockées sur l'instance en faveur des informations d'identification accordées par le rôle dans le profil d'instance. Pour plus d'informations sur les profils d'instance AWS, consultez Rôles IAM pour Amazon EC2 .

Informations d'identification AWS

Champs du formulaire Informations d'identification AWS

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour les informations d'identification AWS.
Actifs	Option pour utiliser les informations d'identification.
ID de clé d'accès	L'**ID de clé d'accès** que vous avez généré sur AWS Management Console, tel que : APIAIOSFODNN7EXAMPLE.
Clé d'accès secrète	**Clé d'accès secrète** que vous avez générée sur AWS Management Console, par exemple : wPalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

Champs de formulaire Informations d'identification du principal du service Azure

Champ	Valeur
Nom	Entrez le nom du principal du service à enregistrer avec l'instance.
ID de locataire et	Collez la valeur **ID de répertoire** Azure à partir du portail Azure dans le champ Gestion cloud **ID de locataire**.
ID client	Collez la valeur **ID d'application** Azure de l'application que vous avez enregistrée dans Azure dans le champ Gestion cloud **ID client**.
Méthode d'authentification	Sélectionnez **Secret client**. **Remarque :** **Assertion du client** n'est pas pris en charge.
Clé secrète	Collez la clé secrète qui a été générée lors de la création du principal du service Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	Ce champ s'affiche lorsque la **Méthode d'authentification** est **Secret client**.

Informations d’identification de l’accord d’entreprise Azure

Les informations d’identification de l’accord d’entreprise Azure sont nécessaires pour la fonctionnalité de facturation fournie par l’application Gestion cloud.

Champs de formulaire Informations d’identification de l’accord d’entreprise Azure

Champ	Description
Nom	Saisissez un nom descriptif.
Numéro d'inscription	Entrez le numéro d’inscription à partir d’Azure.
Clé d'accès	Collez la clé d’accès fournie par Azure.

Informations d’identification de Gestion cloud

Ce type d’informations d’identification est disponible pour Orchestration.

Champs de formulaire Informations d’identification de Gestion cloud

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l’appeler **Cloud Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Type	Spécifiez **AWS**.
Nom d'utilisateur	Entrez le nom d’utilisateur CIM à créer dans la table Informations d’identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Mot de passe	Entrez le mot de passe CIM.
Phrase de sécurité SSH	Saisissez une phrase mémorable pour la génération de clés. Par exemple, vous pouvez indiquer **que vendredi est un bon jour**.
Clé privée SSH	Entrez la clé privée SSH.
Protocole d'authentification	Sélectionnez le protocole d’authentification **MD5**ou **SHA** utilisé pour générer la **clé d’authentification**.
Clé d'authentification	Saisissez une clé d’authentification générée par SSH.
Protocole de confidentialité	Entrez l’un des protocoles de confidentialité suivants qui décrit le chiffrement de la **clé de confidentialité** : • **3DES** pour Triple Data Encryption Standard (DES) • **AES128 pour AES** (Advanced Encryption Standard) avec chiffrement 128 bits • **AES192** pour AES avec chiffrement 192 bits

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire Informations d'identification de Gestion cloud (suite)

Champ	Valeur d'entrée
	• **AES256** pour AES avec chiffrement 256 bits • **DES** pour chiffrement DES hérité
Entrez une clé de confidentialité supplémentaire.	
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
Classification	Entrez la classification de l'application pour la découverte de CI.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification du nœud Cloud Management (CMP)

Les informations d'identification du nœud Gestion cloud (CMP) associent les informations d'identification d'un serveur virtuel que Gestion cloud met en service. L'application Gestion cloud crée automatiquement ces informations d'identification.

Remarque :
Vous devrez peut-être désactiver ces informations d'identification si vous ne souhaitez plus qu'elles soient utilisées, modifier la priorité de l'ordre ou sélectionner un serveur MID autorisé à y accéder. Sinon, vous n'avez pas besoin de créer ou de modifier manuellement ce type d'informations d'identification.

Champs du formulaire Informations d'identification du nœud CMP

Champ	Description
Nom	Nom généré automatiquement en fonction du centre de données où se trouve l'ordinateur virtuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du formulaire Informations d'identification du nœud CMP (suite)

Champ	Description
Actif	Si les informations d'identification sont actives.
Concerne	Choisissez si ces informations d'identification sont disponibles pour un serveur MID spécifique ou pour tous les serveurs MID.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Nom d'utilisateur et mot de passe	Nom d'utilisateur et mot de passe du serveur virtuel.
Phrase de sécurité SSH et clé privée SSH	La clé privée et la phrase de sécurité qui protège la clé si le serveur virtuel l'exige.
Protocole d'authentification et clé d'authentification	La clé privée et la phrase de sécurité qui protège la clé si le serveur virtuel l'exige.
Protocole de confidentialité et clé de confidentialité	Protocole de chiffrement utilisé avec le serveur virtuel et entrez la clé de confidentialité.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.

Informations d'identification de la paire de clés SSH Cloud Management (CMP)

Les paires de clés SSH de Gestion cloud (CMP) stockent les clés que l'application Gestion cloud génère automatiquement lorsque les utilisateurs mettent en service des ressources de pile.

Remarque :
Vous devrez peut-être désactiver ces informations d'identification si vous ne souhaitez plus qu'elles soient utilisées. Sinon, vous n'avez pas besoin de créer ou de modifier manuellement ce type d'informations d'identification.

Champs de formulaire Informations d'identification de paire de clés SSH CMP

Champ	Description
Nom	Nom généré automatiquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire Informations d'identification de paire de clés SSH CMP (suite)

Champ	Description
Actif	Si les informations d'identification sont actives.
Clé publique SSH	La clé publique.
Clé privée SSH	Une clé privée sécurisée qui peut être utilisée à la place d'un mot de passe pour les connexions SSH.

Informations d'identification du référentiel d'images de conteneurs

Les informations d'identification du référentiel d'images de conteneurs gèrent l'accès aux référentiels privés pour l'analyse d'images de conteneurs. Ce type d'informations d'identification est disponible pour Découverte.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type référentiel d'image.

Formulaire Informations d'identification du référentiel d'images de conteneur

Champ	Description
Nom	Nom des informations d'identification affectées par l'utilisateur.
Nom d'utilisateur	Nom d'utilisateur avec des autorisations de lecture pour le référentiel.
Mot de passe	Mot de passe avec autorisations en lecture pour le référentiel.
Référentiel	Nom de domaine complet du référentiel. Par exemple : `docker.io/snow_images`.

Informations d'identification Infoblox

Les informations d'identification Infoblox sont nécessaires pour configurer des pools d'IP (IPAM) dans l'application Cloud Management.

Ces champs sont disponibles sur le formulaire Informations d'identification pour les informations d'identification de type Infoblox.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Concerne	Choisissez si ces informations d'identification sont disponibles pour un serveur MID spécifique ou pour tous les serveurs MID.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Version de wAPI	Entrez la version de wAPI que vous utilisez.
Nom d'utilisateur et mot de passe	Entrez le nom d'utilisateur et le mot de passe InfoBlox.

Informations d'identification JDBC

Le type d'informations d'identification JDBC gère l'accès à une connexion JDBC (Java Database Connectivity). Ce type d'informations d'identification est disponible pour Découverte et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type JDBC.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d'identification JMS

Le type d'informations d'identification JMS gère l'accès à un service de message Java (JMS). Ce type d'informations d'identification est disponible pour Découverte et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d'identification pour JMS.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d’identification OAuth 2.0

Les informations d’identification OAuth 2.0 permettent à ServiceNow d’obtenir l’accès aux comptes d’utilisateurs sur un service HTTP.

Ces champs sont disponibles dans le formulaire Informations d’identification pour OAuth 2.0.

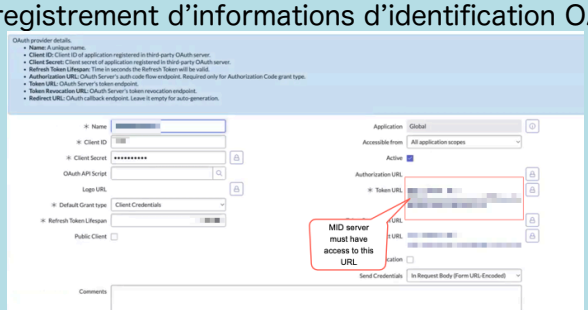
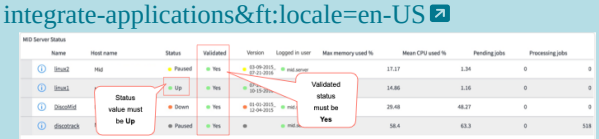
Formulaire Informations d’identification OAuth 2.0

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l’appeler **informations d’identification OAuth2**.
Actif	Indiquez si cet identifiant est actif.
Profil de l'entité OAuth	Un profil OAuth est une combinaison d’un type d’accord et d’au moins un périmètre.
Se connecter au serveur d'authentification via serveur MID	Connecte votre ServiceNow instance à un serveur OAuth sur site qui réside derrière un pare-feu via un Serveur MID. Il peut également connecter votre ServiceNow instance à un serveur OAuth basé sur le cloud via un serveur MID. Lorsque cette option est activée, la demande de jeton OAuth est envoyée via le Serveur MID fichier . **Important :** • L’option s’affiche lorsque la valeur du champ **Type d’accord** du profil d’entité OAuth est définie sur**Informations d’identification** du **client, Code d’autorisation** ou **Informations d’identification du mot de passe du propriétaire de ressource**. Pour savoir comment définir un profil d’entité OAuth pour un fournisseur OAuth tiers, reportez-vous à la section Se connecter à un fournisseur OAuth tiers. • Si vous cochez la case **Se connecter au serveur d’authentification via Serveur MID**, vous devez identifier le ou Serveurs MID dans la liste **S’applique**Serveur MID à.
Concerne	Spécifiez si l’enregistrement des informations d’identification est applicable à tous les serveurs MID ou à un serveur MID spécifique. Si spécifié, ajoutez les MID Server au besoin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
	Important : Assurez-vous de tenir compte de ces considérations si vous avez coché la case **Se connecter au serveur d'authentification via Serveur MID** . • Assurez-vous que toutes les personnes sélectionnées dans S'applique Serveurs MID à peuvent communiquer avec le serveur d'authentification. Cette opération est requise pour exécuter la demande de jeton par rapport à **l'URL de jeton** mentionnée dans l'enregistrement du fournisseur OAuth (qui est liée au profil d'entité OAuth spécifié dans l'enregistrement d'informations d'identification OAuth 2.0).  • Assurez-vous qu'il y en a au moins un (dans la Serveurs MID sélection dans **S'applique**Serveur MID à) avec ces configurations : ◦ La valeur du champ **État** est **Haut**. ◦ La valeur du champ **Validé** est **Oui**. ◦ L'aptitude de est Serveur MID définie sur **REST** ou **TOUT.** Pour en savoir plus sur la configuration du Serveur MID, reportez-vous à la section https://www.webstg.servicenow.com/docs/access?context=configure-capabilities&version=zurich&pubname=zurich-integrate-applications&ft:locale=en-US  . Pour en savoir plus sur ces états, reportez-vous à la section MID Server dashboard .
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
Alias d'identification	Spécifiez l'alias d'informations d'identification que vous souhaitez lier aux informations d'identification OAuth 2.0.
Type d'intégration	Indique le type d'intégration des informations d'identification. Invoquez l'API d'un tiers avec une demande OAuth qui génère un jeton OAuth spécifique au système ou à l'utilisateur. Les types d'intégration sont les suivants : • **Système** : extrayez les informations de jeton en fonction du profil du demandeur. Le type d'intégration **système** prend en charge les mécanismes d'authentification suivants : **1.** SAML (Security Assertion Markup Language) **2.** Jeton Web JSON (JWT) • **Personnel** : extrayez les informations de jeton spécifiques à l'utilisateur. L'utilisateur de Serveur MID doit avoir le rôle `oauth_admin` . Les types **d'intégration Personnel** et **Système** prennent en charge les types d'attribution suivants : **1.** Code d'autorisation **2.** Informations d'identification du mot de passe de propriétaire de ressource Si ce **personnel** est sélectionné sur la page Profil du demandeur OAuth, un marqueur supplémentaire appelé **Personnel** s'affiche. **Remarque :** • Toutes les informations associées à un utilisateur ne sont accessibles qu'avec des jetons OAuth spécifiques à l'utilisateur dont le type d'intégration est **Personnel**. • Pour utiliser le jeton lié à l'utilisateur de la session, vous devez sélectionner le champ **Exécuter en tant que** dans les propriétés du flux en tant **qu'utilisateur qui lance la session**.

Informations d'identification SAP

Le type d'informations d'identification SAP gère l'accès aux systèmes SAP JCo. Ce type d'informations d'identification est disponible pour Découverte et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type SAP.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d'identification SNMP

Découverte explore de nombreux types de périphériques (commutateurs, routeurs, imprimantes, etc.) à l'aide du protocole SNMP. Les informations d'identification pour SNMP n'incluent pas de nom d'utilisateur, seulement un mot de passe, appelé *`chaîne de communauté`*.

La chaîne de communauté en lecture seule par défaut pour de nombreux périphériques SNMP est publique et Découverte l'essaie automatiquement. Entrez les informations d'identification SNMP appropriées si elles sont différentes de la chaîne de communauté *`publique`* .

La détection de SNMP utilise toutes les chaînes de communauté configurées. Ce comportement ne s'applique pas à la détection de SNMPv3.

La requête SNMP d'activité d'orchestration par défaut renvoie l'identificateur d'objet (OID) d'un appareil et requiert des informations d'identification SNMP.

Informations d'identification de la communauté SNMP

Le type d'informations d'identification de la communauté SNMP gère l'accès à la détection de nombreux types d'équipements (commutateurs, routeurs, imprimantes...) à l'aide du protocole SNMP. Ce type d'informations d'identification est disponible pour Découverte, Mappage des services et Orchestration.

Les informations d'identification pour SNMP n'incluent pas de nom d'utilisateur, juste un mot de passe (la chaîne de communauté). La chaîne de communauté en lecture seule par défaut pour de nombreux périphériques SNMP est publique et le système l'essaie automatiquement. Entrez les informations d'identification SNMP appropriées si elles sont différentes de la chaîne de communauté publique.

Ces champs sont disponibles dans le formulaire Informations d'identification pour la communauté SNMP.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d'identification SNMPv3

Les informations d’identification SNMPv3 acceptent un protocole de confidentialité et une clé de confidentialité supplémentaires et sont disponibles pour Détection et Orchestration. Pour le stockage externe dans CyberArk, vous pouvez sélectionner une clé de compte de confidentialité.

Ces champs sont disponibles dans le formulaire Informations d’identification pour SNMPv3.

Champs d'informations d'identification SNMPv3

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **SNMP Community Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu’il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Nom d'utilisateur	Entrez le nom d'utilisateur SNMP. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Protocole d'authentification	Sélectionnez le type d'authentification à utiliser pour ces informations d'identification. Les choix possibles sont les suivants : • MD5 • SHA-1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
	• SHA-224 • SHA-256 • SHA-384 • SHA-512
Clé d'authentification	Entrez la clé d'authentification à utiliser pour ces informations d'identification.
Protocole de confidentialité	Sélectionnez le protocole de chiffrement pour ces informations d'identification. Les choix possibles sont les suivants : • 3DES • AES128 • AES192 • AES256 • DES
Clé de confidentialité	Entrez la clé associée au protocole de confidentialité sélectionné.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un fournisseur d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
ID d'informations d'identification de confidentialité	Entrez la clé de compte de confidentialité configurée pour les informations d'identification SNMPv3 dans CyberArk. Si vous utilisez un protocole de confidentialité dans CyberArk, ce champ doit avoir la même valeur que le champ **Nom** du compte de confidentialité SNMPv3 CyberArk. Ce champ n'est visible que pour SNMPv3 lorsque vous sélectionnez **CyberArk** dans le champ **Type de banque d'identifiants**. Si vous n'utilisez pas de clé de confidentialité pour CyberArk, laissez ce champ vide.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque le stockage externe est activé, le champ **ID d'informations d'identification** s'affiche. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé et que la vue **Stockage externe** est sélectionnée.
Type de banque d'identifiants	Sélectionnez le fournisseur de stockage externe. Sélectionnez **CyberArk** uniquement si vous utilisez une clé de confidentialité SNMPv3 CyberArk. Le champ **ID d'informations d'identification de confidentialité** apparaît pour autoriser l'entrée de la clé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
Contexte d'utilisation	Cochez cette case pour ajouter une valeur de contexte pour ces informations d'identification. Ce champ est visible dans la vue **Discovery**. Les contextes ne sont pas actuellement pris en charge pour le stockage des informations d'identification externe. **Remarque :** Un contexte est une collection d'informations de gestion accessibles par des informations d'identification SNMPv3 qui fait référence à un OID spécifique. Les contextes sont parfois référencés pour collecter des informations sur l'appareil qui ne peuvent pas être consultées par les informations d'identification normales. Un contexte peut être fourni par le fabricant ou être configuré séparément. Si vous avez plusieurs informations d'identification SNMPv3 avec le même nom d'utilisateur et les mêmes clés d'utilisateur, mais que certains de vos appareils ont besoin d'un contexte et d'autres pas, vous devrez créer des enregistrements distincts pour chaque appareil.
Nom de contexte	Entrez la valeur du nom de contexte pour ces informations d'identification. Cette valeur ne doit être utilisée que si vous avez des appareils qui la nécessitent pour un accès complet. Ce champ n'est visible que lorsque la case **Contexte d'utilisation** est cochée.

Informations d'identification SSH

Découverte, Orchestration et Centre d'intégration explorer UNIX et Linux périphériques à l'aide des informations d'identification SSH pour exécuter des commandes sur Secure Shell (SSH). Les commandes SSH doivent s'exécuter avec les privilèges racines, soit avec les informations d'identification racine, soit via Sudo. Les informations d'identification de clé privée SSH fournissent une sécurité supplémentaire.

Octroi des privilèges racines

Avant d'octroyer des privilèges racines, examinez votre politique et vos options de sécurité avec l'équipe de sécurité de votre organisation.

Utilisez l'une ou l'autre de ces approches pour permettre aux utilisateurs d'exécuter des commandes SSH avec des privilèges racines :

- Donnez d'autres informations d'identification pour Découverte, Orchestration ou Centre d'intégration, mais octroyez à l'utilisateur ayant ces informations d'identification le droit d'exécuter certaines commandes avec des privilèges racine, à l'aide de Sudo. Il s'agit d'un moyen sécurisé d'octroyer des privilèges limités. Découverte, Orchestration ou Centre d'intégration utilisent Sudo sur n'importe quelle sonde dont le paramètre `must_sudo` est défini sur **true** (sa valeur par défaut est **false**). Toutefois, chaque système doit être configuré pour permettre à Sudo de fonctionner. Pour ce faire, modifiez le fichier **/etc/sudoers** à l'aide de la commande **visudo**.
- Donnez les informations d'identification **racine**. Il s'agit bien entendu des informations d'identification les plus puissantes, mais elles ne sont pas toujours souhaitables pour des raisons de sécurité. Si Découverte, Orchestration ou Centre d'intégration ont les informations d'identification racine pour n'importe quel système UNIX ou Linux, aucune autre configuration n'est nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes privilégiées

La plateforme fournit des commandes privilégiées par défaut que le MID Server doit utiliser et la possibilité d'ajouter des commandes supplémentaires au système. Pour plus d'informations sur l'utilisation de sudo et d'autres commandes privilégiées, consultez Commandes privilégiées de Serveur MID .

Type d'informations d'identification de clé privée SSH

Remarque :
Les informations d'identification de clé privée SSH doivent être utilisées dans la plupart des cas. Ils offrent une meilleure sécurité que les identifiants de mot de passe SSH, y compris contre les attaques MitM (man-in-the-middle) dans lesquelles les communications entre deux parties sont interceptées.

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez les appeler **SSH Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez un nom d'utilisateur UNIX ou Linux. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Mot de passe	Entrez le mot de passe UNIX ou Linux. Pour les informations d'identification de type **Clé privée SSH** , entrez le mot de passe Sudo si le nom d'utilisateur en nécessite un.
Phrase de sécurité SSH	Saisissez une phrase de sécurité SSH. Ce champ est disponible uniquement pour les informations d'identification de **Clé privée SSH** .

Clé privée SSH	Saisissez une clé privée sécurisée, RSA, DSA, ECDSA ou ED25519.
	La clé privée doit être saisie au bon format pour être correctement chiffrée. La clé privée doit commencer par la chaîne -----BEGIN.
	Voici un exemple de clé privée RSA correctement formatée :
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END RSA PRIVATE KEY-----`
	Un exemple de clé DSA :
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END DSA PRIVATE KEY-----`
	Un exemple de clé ECDSA :
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END EC PRIVATE KEY-----`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur d'entrée
	Et un exemple de clé privée ED25519 : -----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW QyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lllq/aE66mufmiwAAAKDQUtxZ0FLc WQAAAAtzc2gtZWQyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lllq/aE66mufmiw AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSViWqFx3DHxVDNnIdogLmW1 CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTUE3OTAzMkI3AQID -----END OPENSSH PRIVATE KEY----- **Remarque :** Pour une clé privée ED25519, seul le format de clé OpenSSH est pris en charge, qui est généré à l'aide de l'utilitaire OpenSSH SSH-keygen. Le ServiceNow AI Platform prend en charge les clés privées au format PEM généré par l'utilitaire OpenSSH ssh-keygen. Pour convertir les clés PPK qui ont été générées par PuTTY : • Ouvrez votre clé privée dans PuTTYGen. • Exportez-le au format OpenSSH depuis le menu **Conversions** > **Exporter une clé OpenSSH**. • Enregistrez la nouvelle clé OpenSSH.
Certificat SSH	Entrez un certificat OpenSSH basé sur RSA ou ED25519. Lorsque le certificat est saisi, une clé privée est utilisée pour l'authentification basée sur certificat. Cette authentification est prise en charge à partir d'OpenSSH 7.8.
Alias d'identification	• Autorisez les concepteurs de flux à utiliser des alias pour gérer les connexions et les informations d'identification. L'utilisation d'un alias élimine la nécessité de configurer plusieurs informations d'identification et profils d'informations de connexion lors de l'utilisation d'environnements multiples. Si les informations de connexion ou d'identification changent, vous n'avez pas besoin de mettre à jour les actions qui utilisent la connexion. Pour plus d'informations, consultez Connexions et informations d'identification. • Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur d'entrée
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
Ordre	Ordre (séquence) dans lequel la plateforme essaie ces informations d'identification lorsqu'elle tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des numéros élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), Discovery ou Orchestration essaie les informations d'identification aléatoirement.

Type d'informations d'identification SSH

Ces champs sont disponibles dans le formulaire Informations d'identification SSH.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	• Autorisez les concepteurs de flux à utiliser des alias pour gérer les connexions et les informations d'identification. L'utilisation d'un alias élimine la nécessité de configurer plusieurs informations d'identification et profils d'informations de connexion lors de l'utilisation d'environnements multiples. Si les informations de connexion ou d'identification changent, vous n'avez pas besoin de mettre à jour les actions qui utilisent la connexion. Pour plus d'informations, consultez Connexions et informations d'identification. • Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d'identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Commandes qui nécessitent des privilèges racine pour Discovery, Orchestration et Centre d'intégration

Dans ces exemples, le nom d'utilisateur est **Disco**. Remplacez le nom d'utilisateur et assurez-vous que les chemins d'accès des commandes correspondent aux chemins d'accès du système.

Remarque :
Les commandes Sudo ne fonctionnent pas avec les informations d'identification de clé privée, car il n'y a pas de mot de passe à fournir à la commande Sudo. Une solution consiste à ajouter l'option *NOPASSWD* à la configuration Sudo. Par exemple, vous pouvez entrer : `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

Commandes UNIX et Linux nécessitant des privilèges racine

Commande	Objectif
HP-UX	
adb	Collecte la vitesse et la mémoire du processeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
	• **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/adb • **Utilisée par** : Discovery
Toutes les versions Linux et UNIX	
chage	Modifie le nombre de jours entre les changements de mot de passe et la date du dernier changement de mot de passe. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/chage • **Utilisée par** : Orchestration et Centre d'intégration
chpasswd	Modifie les mots de passe utilisateur. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/chpasswd • **Utilisée par** : Orchestration et Centre d'intégration
Toutes les versions Linux	
dmidecode	Collecte différentes informations sur le matériel, y compris le numéro de série incorporé dans la carte mère. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/dmidecode • **Utilisée par** : Discovery
fdisk	Collecte les informations sur les disques et la taille sur le système. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/fdisk -l • **Utilisée par** : Discovery
multipath	Collecte les mappages d'appareils pour le MPIO. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/multipath -ll • **Utilisée par** : Discovery
ls	Rassemble le contenu d’un répertoire. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/ls, /bin/ls • **Utilisée par** : Discovery
Linux et Solaris	
dmsetup	Examine un volume de faible niveau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif

	• **Exemple de ligne de /etc/sudoers** :
	  ○ Disco ALL=(root) /usr/bin/dmsetup table *
	  ○ Disco ALL=(root) /usr/bin/dmsetup ls
	• **Utilisée par** : Discovery

Toutes les versions UNIX	
lsof	Détermine la relation entre les processus et les connexions en cours au système. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /sbin/lsof • **Utilisée par** : Discovery
oratab	Accorde un accès en lecture au fichier oratab pour localiser la page d'accueil et le profil Oracle. • **Exemple de ligne /etc/sudoers** : N. A. • **Utilisée par** : Discovery
Solaris	
iscsiadm	Obtient des IQN iSCSI • **Exemple de ligne /etc/sudoers** : ${sudo:iscsiadm list target -S} • **Utilisée par** : Discovery
fcinfo	Obtient des WWPN pour les ports. • **Exemple de ligne /etc/sudoers** : ${sudo:fcinfo remote-port -sl -p $port} • **Utilisée par** : Discovery
prtvtoc	Communique des informations sur les partitions de disque. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/prtvtoc • **Utilisée par** : Discovery
pfiles	Utilisé pour collecter des informations de connexion TCP. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/pfiles • **Utilisée par** : Discovery

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
PGREP	Utilisé pour répertorier les ID de processus d'une région particulière sur lesquels exécuter des fichiers. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/pgrep • **Utilisée par** : Discovery
/usr/bin/ps	Répertorie le processus d'exécution. Vous pouvez ajouter le rôle proc_owner au lieu de l'exécuter avec l'accès racine. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/ps • **Utilisée par** : Discovery
/usr/ucb/ps	Répertorie le processus d'exécution. Vous pouvez ajouter le rôle proc_owner au lieu de l'exécuter avec l'accès racine. L'utilisation de la commande `/usr/ucb/ps` est déconseillée à partir de Solaris 11. Étant donné que Découverte, Orchestration et Centre d'intégration nécessitent l'utilisation de cette commande pour toutes les versions Solaris, vous devez installer l'utilitaire ucb manuellement sur les systèmes Solaris 11. Pour obtenir des instructions, consultez KB0564262 . • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/ucb/ps • **Utilisée par** : Discovery

Pour obtenir la liste des commandes privilégiées dont vous avez besoin pour Détection et Mappage des services, reportez-vous à la section Service Mapping commands requiring a privileged user . Cette liste inclut les commandes qui nécessitent des droits élevés pour détecter et mapper les hôtes Unix dans votre organisation.

Besoins relatifs à l'accès pour les informations d'identification non racine

Si vous ne fournissez pas d'informations d'identification Découverte avec accès racine, vous devez fournir les informations d'identification avec les besoins relatifs à l'accès suivantes.

Application	Fichier ou répertoire	Accès requis
Apache	httpd.conf	Lecture
HBase	hbase-site.xml	Lecture
JBoss	jboss-service.xml	Lecture
	Répertoire de base JBoss	Lecture
	web.xml	Lecture
MySQL	my.cnf	Lecture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Fichier ou répertoire	Accès requis
NGINX	nginx.conf	Lecture
Oracle	oratab	Lecture
	Fichiers pfiles (s) associés	Lecture
Oracle Listener	lsnrctl	Exécuter
	listener.ora	Lecture
Tomcat	catalina.jar	Lecture
	server.xml	Lecture
	web.xml	Lecture
Unix	/etc/*release	Lecture
	/etc/bashrc	Lecture
	/etc/profile	Lecture
	/proc/cpuinfo	Lecture
	/proc/vmware/sched/ncpus	Lecture
	/var/log/dmesg	Lecture
	Répertoire APD	Lecture
WebSphere	cell.xml	Lecture
	server.xml	Lecture
	serverindex.xml	Lecture

Informations d'identification VMware

Le type d’informations d’identification VMware gère l’accès aux informations d’identification vCenter.

Les applications qui accèdent aux ressources dans le cloud VMware ont besoin d'accéder aux informations d'identification VMware. Par exemple, le type d’informations d’identification VMware permet à Découverte d’explorer vCenter de VMware exécuté sur un ordinateur Windows pour détecter les machines ESX, les ordinateurs virtuels et les pools de ressources. L’API VMware Découverte et d’automatisation (API vCenter) fournit désormais le numéro de série unique au niveau mondial pour les CI d’ordinateur. Les informations d’identification CIM ne sont pas nécessaires pour activer l’accès à chaque hôte VMware.

Remarque :
Les informations d’identification Windows ne sont pas nécessaires pour vCenter Découverte, lorsque des informations d’identification VMware valides sont utilisées.

Important :
N’utilisez pas les informations d’identification **de type VMware** pour les activités Orchestration qui exécutent des travaux sur les ordinateurs virtuels individuels clonés par vCenter (par exemple, le redémarrage d’un ordinateur virtuel Linux). Pour ces activités, le **type** d’informations d’identification dépend du système d’exploitation de l’ordinateur virtuel (**SSH** ou **Windows**).

Formulaire Informations d'identification VMware

Champ	Description
Nom	Entrez un nom unique et descriptif pour les informations d'identification VMware.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification VMware (suite)

Champ	Description
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur que vous utilisez pour votre compte VMware. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Les informations d'identification VMware doivent avoir un rôle en lecture seule dans vCenter.
Mot de passe	Entrez le mot de passe du compte VMware.
Concerne	Sélectionnez-en un ou plusieurs Serveurs MID dans la liste des fichiers .Serveurs MID Les informations d'identification Serveurs MID configurées dans cet enregistrement sont disponibles dans cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification Windows

Les informations d'identification Windows permettent d'accéder aux ordinateurs Windows. Ce type d'informations d'identification est disponible pour Découverte et Orchestration.

Exigences en matière d'informations d'identification

Découverte et Orchestration ont les exigences suivantes en matière Windows d'informations d'identification :

- Installez un Serveur MID sur un Windows hôte en tant que service.
- Ajoutez Windows des informations d'identification à l'un de ces emplacements :
  - Une entrée dans la table Informations d'identification [windows_credentials]
  - Compte de service Serveur MID à exécuter en tant qu'utilisateur Windows ou compte de domaine spécifique.

Octroi des autorisations appropriées

Pour fournir des autorisations suffisantes, Windows les informations d'identification doivent être l'une des suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- un utilisateur de domaine avec un accès administrateur local sur les hôtes Windows cibles ;
- Compte local disposant de privilèges d'administrateur et du contrôle d'accès utilisateur (UAC) désactivés sur le même hôte cible.
- Utilisateur qui répond aux exigences de Windows sondes et d'autorisations (Découverte uniquement).
- Un utilisateur qui répond aux exigences de l'activité Orchestration à exécuter (Orchestration uniquement).

Remarque :
Aucun privilège de connexion n'est nécessaire. Le compte n'a PAS besoin d'être interactif.

La sécurité autour de l'octroi d'un accès privilégié peut être renforcée à l'aide des profils JEA pour s'exécuter Découverte. Pour plus d'informations, consultez Microsoft Just Enough Administration (JEA) pour Discovery .

Ordinateurs des groupes de travail

Pour exécuter les commandes Powershell afin de détecter un ordinateur de groupe de travail, configurez les informations d'identification du serveur MID pour l'un de ces utilisateurs :

- Compte administrateur intégré sur l'ordinateur du groupe de travail.
- Utilisateur du domaine sur l'ordinateur du groupe de travail.

Configuration multi-domaine

Pour activer les informations d'identification Windows à fonctionner sur plusieurs domaines, assurez-vous d'utiliser les formats de nom et la configuration du serveur MID corrects.

Découverte et les informations d'identification de domaine de prise en charge Windows**d'Orchestration dans les formats de nom d'utilisateur Nom principal de l'utilisateur** et **Nom de connexion de bas niveau** . Par exemple, **Domaine\Nom d'utilisateur** ou **UserName@example.domain.com**. Vous pouvez fournir Windows les informations d'identification du groupe de travail au format suivant : WORKGROUP\UserName.

Remarque :
Vous pouvez également fournir un compte local à l'aide du nom d'utilisateur **.** .

Ces actions supplémentaires sont nécessaires pour permettre aux informations d'identification de fonctionner dans plusieurs Windows domaines.

Condition	Actions supplémentaires requises
Hôte du Serveur MID sur le même domaine que la Windows cible.	Aucun
Hôte du Serveur MID sur un domaine différent de la Windows cible.	Assurez-vous que PowerShell 3.0 (ou une version ultérieure jusqu'à la version 5.1) est installé sur l'hôte du Serveur MID.
Hôte du Serveur MID sur un domaine différent de la cible Microsoft SQL Server.	Voir Détection de serveur MSSQL .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d’informations d’identification Windows

Ces champs sont disponibles dans le formulaire Informations d’identification pour Windows :

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d’identification externe n’est disponible que lorsque le module d’extension Stockage des informations d’identification externe est activé. **Remarque :** Actuellement, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les utilisateurs qui doivent utiliser ces informations d’identification Serveurs MID dans le champ **Serveurs MID** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est uniquement utilisé pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Les MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste cet identifiant de connexion lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Configurer les informations d'identification Windows pour le serveur MID

Configurez le Serveur MID pour qu'il utilise les informations d'identification de son propre service Windows ou les informations d'identification de la table Informations d'identification [discovery_credentials].

Avant de commencer

Rôle requis : admin

Procédure

1. Configurez le serveur MID pour utiliser les informations d'identification du compte de service de serveur MID.
   a. Définissez les informations d'identification de service Configurer Windows MID Server sur un utilisateur qui répond aux besoins d'autorisation.
   b. Vérifiez que le nom d'utilisateur répond aux exigences de format de nom.
   c. Renseignez les champs du formulaire comme il convient.
   d. Vérifiez que les informations d'identification répondent aux exigences du domaine.
2. Configurez Serveur MID Utilisez les informations d'identification à partir de la table Informations d'identification [discovery_credentials].
   a. Ajouter des informations d'identification individuelles Windows à la table Informations d'identification [windows_credentials].
      - Vérifiez que chaque information d'identification répond aux exigences d'autorisation.
      - Vérifiez que chaque nom d'utilisateur répond aux exigences de format de nom.
      - Vérifiez que chaque information d'identification répond aux exigences du Windows domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Facultatif : Configurez le Serveur MID pour utiliser Powershell en définissant le paramètre `mid.use_powershell` sur **vrai**.
Voir Configuration des serveurs MID .

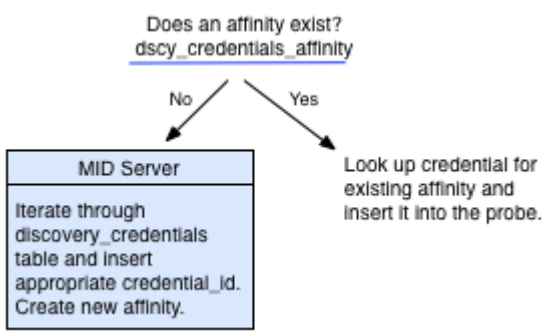
c. Cochez la case Compte de service Windows MID Server pour créer une information d'identification qui représente le compte de service Windows MID Server à exécuter en tant qu'utilisateur Windows ou compte de domaine spécifique.

Relation d'informations d'identification pour Découverte et Orchestration

L'affinité d'informations d'identification est une association entre un ensemble d'informations d'identification et un appareil de votre réseau.

Lorsque Découverte Notre Orchestration tente pour la première fois d'accéder à un appareil, ils essaient toutes les informations d'identification disponibles jusqu'à ce qu'ils trouvent les bonnes. Après avoir identifié les informations d'identification d'un appareil et Orchestration, Découverte créez une relation entre les informations d'identification et l'appareil à l'aide de la table Relation d'informations d'identification [dscy_credentials_affinity]. Toutes les détections ultérieures ou les activités d'Orchestration tentent de faire correspondre les informations d'identification de cette table à un appareil pour lequel il existe une relation. Si les informations d'identification d'un périphérique changent, Découverte Orchestration réessaie toutes les informations d'identification disponibles jusqu'à ce qu'elles créent une nouvelle relation.

Diagramme de relation des informations d'identification



Remarque :
Si Orchestration est Découverte installé, et que l'alias d'informations d'identification est activé, plusieurs relations peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification pour chaque relation et insère les informations d'identification de la relation avec l'ordre le plus bas dans la sonde.

Dépannage des informations d'identification

Passez en revue la section `<credentials_debug>` de la charge utile de la file d'attente ECC pour résoudre les problèmes d'informations d'identification.

Certaines sondes prennent en charge le débogage des informations d'identification. Le débogage des informations d'identification insère une section `<credentials_debug>` dans la charge utile que le MID Server renvoie à la file d'attente ECC de l'instance. Vous pouvez consulter la section `<credentials_debug>` pour afficher des informations détaillées sur la recherche d'informations d'identification.

La section `<credentials_debug>` apparaît dans la charge utile si :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les informations d'identification de la sonde WMIRunner, de la sonde PowerShell, de la sonde JMS ou SSHCommand échouent.
- Vous définissez le *credentials_debug* paramètre sur **true** pour les sondes WMIRunner, PowerShell ou SSHCommand. Si vous définissez le paramètre sur vrai, la section <credentials_debug> s'affiche même si la recherche d'informations d'identification réussit.

La section <credentials_debug> affiche :

- Informations sur la recherche d'informations d'identification, telles que les types d'informations d'identification, les balises et les relations.
- Adresse IP ciblée.
- Informations sur chaque identifiant (dans l'ordre) utilisé par le Serveur MID, y compris le type, la classification, la balise, le nom, l'ID système et l'ID d'identifiant d'identification externe, le cas échéant.

Exemple de charge utile montrant des informations d'identification non valides

Payload XML


```
<?xml version="1.0" encoding="UTF-8"?><results probe_time="6891" result_code="0"><result
id="6f10ed420a0a0b7e49052d83a32b586f" name="sh ${file:esx.sh}" order="1" topic="SSHCommand"><results
error="SSHCommand: Adding target to blacklist.  No valid credential found for types [SSH Password,SSH
Private Key]" probe_time="6860" result_code="42"><result error="SSHCommand: Adding target to blacklist.
No valid credential found for types [SSH Password,SSH Private Key]"><debug_info>{"debug_info":
[{"10.11.129.81":{"credentials_attempted":[{"credential_type":"SSH
Password","credential_name":"badCredential1","credential_order":"100","credential_success":false,"credenti
al_id":"6b43751d1362a200efffb6004244b0c3"},{"credential_type":"SSH
Password","credential_name":"badCredential2","credential_order":"200","credential_success":false,"credenti
al_id":"1553b11d1362a200efffb6004244b01b"},{"credential_type":"SSH
Password","credential_name":"badCredential3","credential_order":"300","credential_success":false,"credenti
al_id":"7d63f11d1362a200efffb6004244b0b0"}],"adding_key_to_target_blacklist":true,"connection_parameters":
{"credential_types":["SSH Password","SSH Private Key"],"target":"10.11.129.81"}}}]}</debug_info></result>
<parameters><parameter name="discover" value="CIs"/><parameter name="agent"
value="mid.server.demonightlyIstanbul_MID"/><parameter name="glide.xmlhelper.trim.enable" value="true"/>
<parameter name="use_class" value="discovery_classy_unix"/><parameter name="source" value="10.11.129.81"/>
<parameter name="priority" value="0"/><parameter name="use_snc_ssh" value="true"/><parameter name="probe"
value="10e0eebd0a0a0b4f61f46a5027df7fb6"/><parameter name="port_probe"
value="97ff2abd0a0a070300b7f37daa11a241"/><parameter name="port" value="22"/><parameter name="cidata"
value="&lt;CIData&gt;&lt;data&gt;&lt;fld name=&quot;ip_address&quot;&gt;10.11.129.81&lt;/fld&gt;&lt;/data&
gt;&lt;/CIData&gt;"/><parameter name="used_by_discovery" value="true"/><parameter name="name" value="sh
${file:esx.sh}"/><parameter name="topic" value="SSHCommand"/><parameter name="esx.sh" value="#!/bin
/sh&#13;&#10;# This command is rarely installed, so a Bourne shell script is used to squelch the exit
status and sensor warning when not found.&#13;&#10;# tcsh doesn't squelch exist status codes within
backticked statements&#13;&#10;echo `vmware -v 2&gt;&amp;1`"/><parameter name="ecc_queue" value=""/>
</parameters></results></result><result id="e5e075a2a9fe1561018f2a9636d5ec39" name="uname -a" order="1"
topic="SSHCommand"><results error="SSHCommand: Target is blacklisted.  No valid credential found for
```


Les détails du paramètre PowerShell s'affichent :

- Si les informations d'identification du serveur MID local ont été utilisées après l'échec de toutes les informations d'identification Windows.
- Si les informations d'identification ont été ignorées parce que vous essayez de détecter le même ordinateur que le serveur MID.
- Si le paramètre mid.powershell.use_credentials est défini sur true.

Les détails apparaissent pour le SSHCommand :

- Si la recherche d'informations d'identification a été ignorée car l'adresse IP cible est exclue.
- Si l'adresse IP cible a été ajoutée à la liste d'exclusion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le Serveur MID enregistre les adresses IP des recherches d'informations d'identification ayant échoué dans une liste d'exclusion dans la mémoire cache. Cette liste d'exclusion spécifie les équipements auxquels le serveur MID doit cesser d'essayer d'accéder. Les adresses IP sont ajoutées à la liste d'exclusion après l'échec de chaque information d'identification. Les adresses IP sont effacées du cache de la liste d'exclusion au bout de cinq minutes, si le serveur MID est redémarré ou si les enregistrements d'informations d'identification sur l'instance sont mis à jour.

Stockage externe des informations d'identification

Une instance peut stocker les informations d'identification utilisées par Découverte, Orchestration et Mappage des services dans un référentiel d'informations d'identification externe plutôt que directement dans un enregistrement d'informations d'identification ServiceNow .

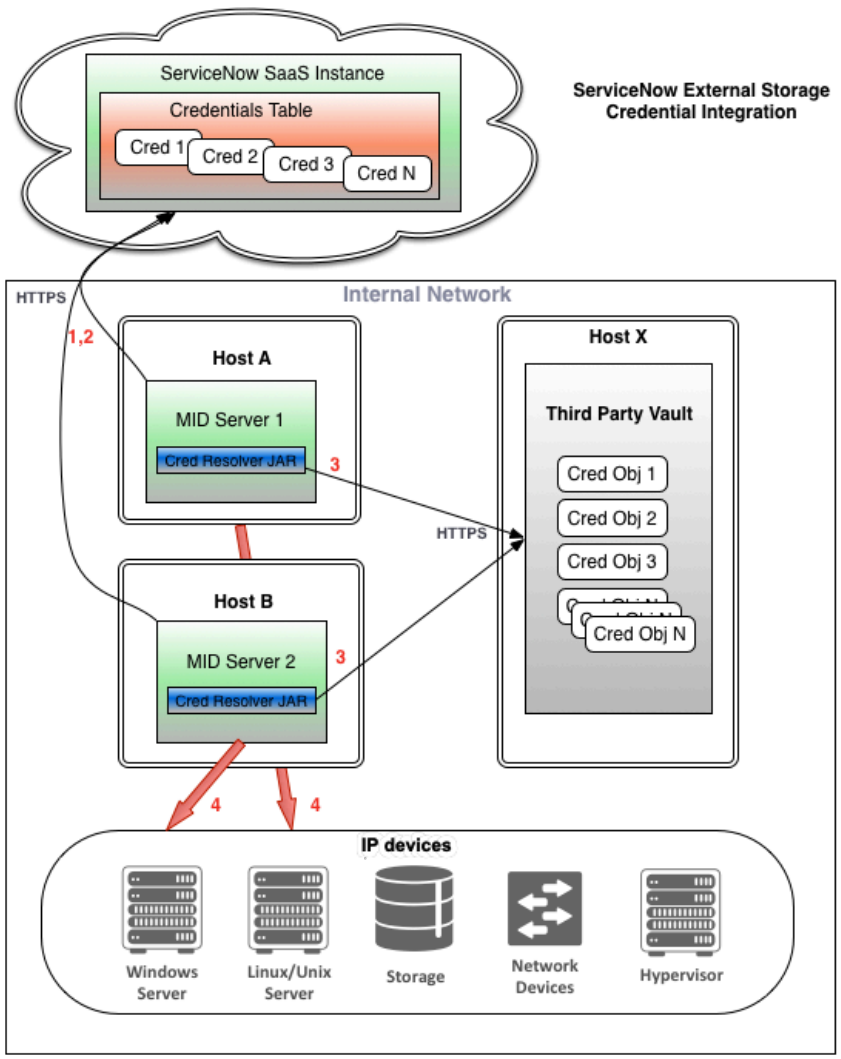
L'instance gère un identificateur unique pour chaque information d'identification, le type d'information d'identification (SSH, SNMP ou Windows, par exemple) et toutes les relations d'identification. Le Serveur MID obtient l'identificateur d'informations d'identification à partir de l'instance, puis utilise un fichier JAR fourni par le client pour résoudre l'identificateur du référentiel en informations d'identification utilisables. Actuellement, la ServiceNow® plateforme prend en charge l'utilisation du coffre-fort CyberArk ou de BeyondTrust pour le stockage d'informations d'identification externes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture de stockage des informations d'identification externe

Architecture de stockage des informations d'identification externe



Flux de processus des informations d'identification

Le Serveur MID récupère les informations d'identification d'une banque externe à l'aide du processus suivant :

1. Serveur MID télécharge les objets d'informations d'identification de la ServiceNow table Informations d'identification [discovery_credentials] contenant l'ID d'informations d'identification correspondant du coffre cible.
2. Au fur et à mesure que chaque sonde ou modèle s'exécute à partir de Découverte ou Orchestration de tâches, le serveur MID demande les informations d'identification en transmettant des informations telles que l'ID d'informations d'identification, l'adresse IP cible et le type d'informations d'identification au fichier jar Java pour le programme de résolution des informations d'identification. Les détails de l'objet d'informations d'identification correct à récupérer dans le coffre sont déterminés par le programme de résolution des informations d'identification.

   De nombreux résolveurs d'informations d'identification tels que CyberArk appellent une application fournie par le fournisseur de coffre-fort tiers fonctionnant sur la même machine que le MID Server. Cette application peut souvent être configurée pour mettre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en cache les informations d'identification et sait mettre à jour le cache lorsqu'une information d'identification change dans le coffre, ce qui est très important pour éviter les appels réseau inutiles vers le coffre chaque fois que le MID Server demande un identifiant. Le résolveur d'informations d'identification (à l'aide de l'application du fournisseur facultative le cas échéant) appelle le coffre-fort pour obtenir le nom d'utilisateur, le mot de passe, etc.

Pour les résolveurs d'informations d'identification fournis prêts à l'emploi (uniquement CyberArk aujourd'hui), le MID Server ne met en cache les informations d'identification que pendant plusieurs secondes à l'aide du chiffrement dans la mémoire de processus du MID Server. Cela signifie que le Serveur MID peut effectuer plusieurs demandes au programme de résolution des informations d'identification pour les mêmes informations d'identification, même lors de la détection d'un seul appareil. Contactez les fournisseurs tiers pour plus d'informations sur les implémentations de mise en cache pour d'autres Résolveurs d'informations d'identification.

3. Serveur MID exécute la sonde avec les informations d'identification appropriées.

Remarque :
L'affinité des titres de compétences s'applique toujours. Le mécanisme reste le même, car la seule véritable différence du point de vue du MID Server est que les véritables détails des informations d'identification (nom d'utilisateur et mot de passe) proviennent du coffre-fort tiers.

Journalisation du stockage des informations d'identification externe

Le serveur MID publie des messages de journal sur le stockage des identifiants externes.

Si le référentiel rencontre une erreur lors d'une tentative de résolution d'une demande d'informations d'identification, le MID Server publie des messages de journal avec le préfixe Problem with client's CredentialResolver:

Composants installés avec le stockage d'informations d'identification externe

Business Rule

La règle métier Stockage des informations d'identification externe effectue les tâches suivantes lorsqu'un administrateur modifie la propriété Activer le stockage des informations d'identification externe :

- Elle remplace la vue de la liste et du formulaire d'enregistrement Informations d'identification par la vue Stockage externe. Cette vue permet aux utilisateurs d'afficher la colonne **ID d'informations d'identification** dans la liste.
- Elle indique au MID Server d'actualiser son cache d'informations d'identification en vue de changer la façon dont les informations d'identification sont obtenues.

Propriété

Une propriété appelée Activer le stockage des informations d'identification externe [com.snc.use_external_credentials] active ou désactive le module d'extension Stockage des informations d'identification externe une fois qu'il est activé. La propriété est située à **Définition de découverte** > **Propriétés** et **Orchestration** > **Propriétés de serveur MID**et est activé lorsque vous activez le module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous désactivez le stockage des informations d'identification externe avec la propriété système, le système définit automatiquement toutes les informations d'identification externe comme inactives dans l'instance. Si vous réactivez la fonctionnalité avec cette propriété, le système ne réinitialise pas les enregistrements d'informations d'identification externes sur actif. Vous devez réactiver manuellement chaque enregistrement d'informations d'identification.

Demander un stockage d'informations d'identification externe pour Découverte et Orchestration

Le module d'extension Stockage des informations d'identification externe est disponible à la demande.

Avant de commencer

Rôle requis : admin

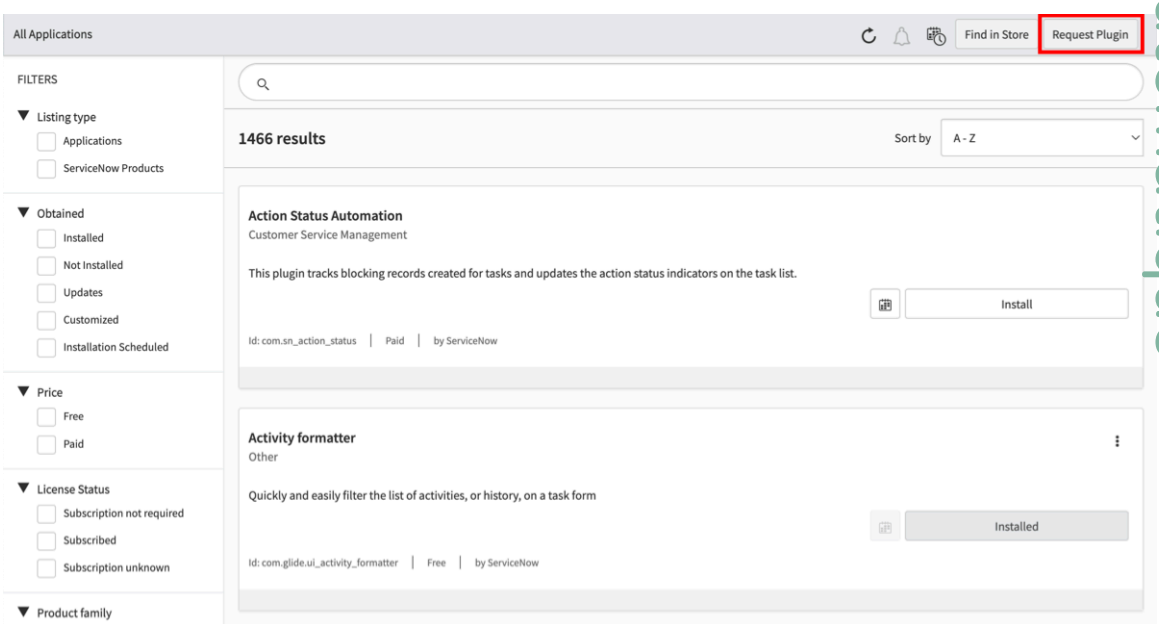
Pourquoi et quand exécuter cette tâche

Il existe deux façons de demander un module d'extension :

- Accéder directement au Now Support catalogue de services en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

Procédure

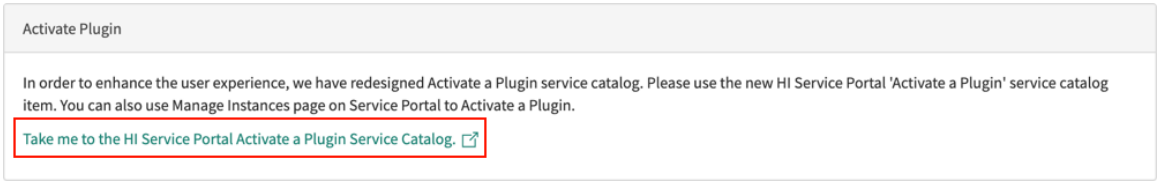
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

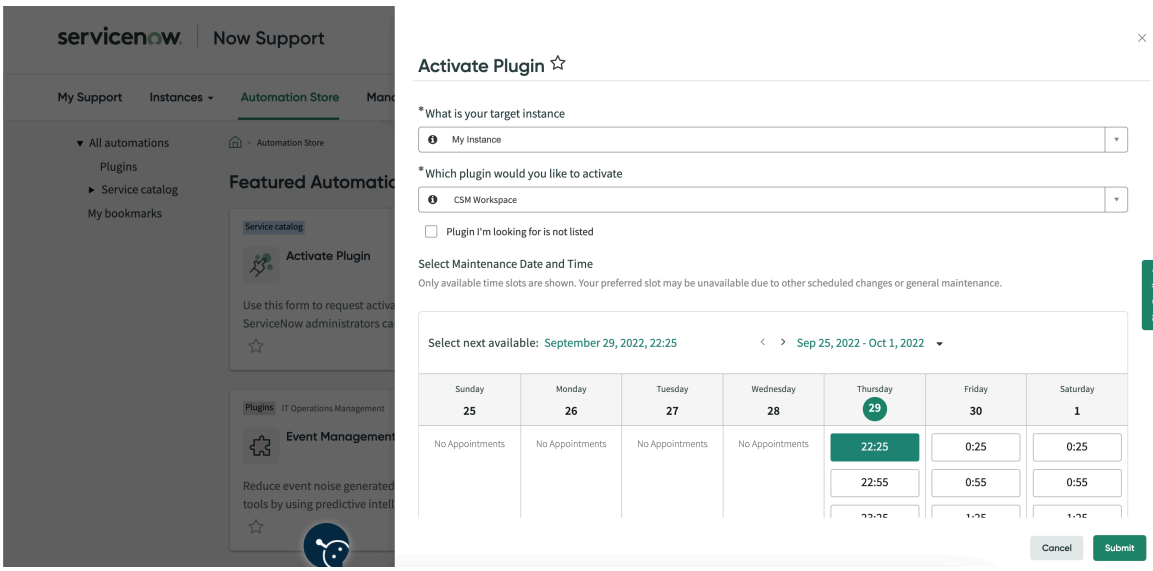
Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Activer le module d'extension



7. Sélectionnez **Soumettre**.
Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Configuration du stockage des informations d'identification externe

Configurez votre instance pour obtenir les informations d'identification à partir d'un référentiel distant.

Ces procédures supposent que vous disposez déjà d'un référentiel externe configuré avec les informations d'identification que vous souhaitez protéger. L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé aux informations d'identification réelles dans le référentiel via le fichier JAR.

Remarque :
ServiceNow prend en charge deux coffres-forts externes à la fois : un outil de résolution des informations d'identification CyberArk par défaut et un outil de résolution des informations d'identification externe personnalisé. La création d'un outil de résolution des informations d'identification CyberArk personnalisé utilise toujours le deuxième coffre externe personnalisé, et aucun coffre externe personnalisé supplémentaire ne peut être utilisé.

Pour configurer le stockage des informations d'identification externe, effectuez les tâches suivantes dans l'ordre.

Créer un fichier JAR pour résoudre les informations d'identification

Créez un fichier JAR pour résoudre les identificateurs d'informations d'identification envoyés par le serveur MID en informations d'identification réelles du référentiel.

Avant de commencer
Rôle requis : agent_admin ou admin

Assurez-vous d'inclure tous les éléments d'informations d'identification attendus par l'instance, tels que la clé privée.

Pour créer un fichier JAR afin de résoudre les informations d'identification :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Utilisez les modèles fournis sur GitHub ServiceNow ou l'exemple de fichier Java.

> **ATTENTION :**
> Ces exemples sont destinés à servir de modèle uniquement. N'utilisez **PAS** ce code en production sans le modifier pour votre environnement.

a. Téléchargez les fichiers JAR open source avec les instructions de github ServiceNow :

- Outil de résolution des informations d'identification externes HashiCorp
- Outil de résolution des informations d'identification externes CyberArk

b. Utilisez l'exemple de fichier Java suivant comme modèle et modifiez-le en fonction de votre environnement :

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH = "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
// the string password for the credential, if needed...
public static final String VAL_PSWD = "pswd";

// the string pass phrase for the credential if needed:
public static final String VAL_PASSPHRASE = "passphrase";

// the string private key for the credential, if needed...
public static final String VAL_PKEY = "pkey";

// the string authentication protocol for the credential, if needed...
public static final String VAL_AUTHPROTO = "authprotocol";

// the string authentication key for the credential, if needed...
public static final String VAL_AUTHKEY = "authkey";

// the string privacy protocol for the credential, if needed...
public static final String VAL_PRIVPROTO = "privprotocol";

// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using default file:
"+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycred
entials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}

 /**
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 * Resolve a credential.
 */
public Map resolve(Map args) {
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
 result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
 result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
 result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
 result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
 result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

 System.err.println("Error while resolving credential id/type["+id+"/"+type+"]");

 return result;
}


/**
 * Return the API version supported by this class.
 */
public String getVersion() {
 return "1.0";
}

public static void main(String[] args) {
 CredentialResolver obj = new CredentialResolver();
 obj.loadProps();

 System.err.println("I spy the following credentials: ");
 for(Object key: obj.fProps.keySet()) {
  System.err.println(key+": "+obj.fProps.get(key));
 }

 }
}
```

Importer un fichier JAR pour résoudre les informations d'identification

Importez un fichier JAR créé pour résoudre les identificateurs d'identification envoyés par Serveur MID en informations d'identification réelles du référentiel.

Avant de commencer
Rôle requis : agent_admin ou admin

Une fois le fichier JAR créé, importez-le dans l'instance, où il devient accessible au serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Après avoir créé le fichier JAR et les fichiers de propriétés, copiez le fichier de propriétés sur Serveur MID.
2. Accédez à la **Serveur MID** > **Fichiers JAR**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs suivants :

Champ	Description
Nom	Nom unique et descriptif permettant d'identifier le fichier dans l'instance.
Version	Numéro de version du fichier, le cas échéant.
Source	Emplacement du fichier JAR à des fins de référence. Les informations sources ne sont pas utilisées par le système.
Description	Brève description du fichier JAR et de son objectif dans l'instance.

5. Cliquez sur l'icône du presse-papier dans la bannière et joignez le fichier JAR à l'enregistrement.

Example



6. Cliquez sur **Envoyer**.
7. Redémarrez le service Serveur MID.
   La plateforme met le fichier JAR à la disposition de tout serveur MID configuré pour communiquer avec l'instance.

Configurer l'identificateur d'informations d'identification

Configurez l'identificateur d'informations d'identification dans l'instance.

Avant de commencer

Rôle requis : admin

Vérifiez les éléments suivants :

- Le module d'extension Stockage des informations d'identification externe doit être actif.
- La propriété Activer la découverte du stockage des informations d'identification externe est activée.

Procédure

1. Accédez à la **Tous** > **Découverte** > **Informations d'identification** ou **Orchestration** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez un type d'informations d'identification.
4. Sélectionnez la case à cocher **Banque d'identifiants externes** .
   Les champs **Nom d'utilisateur** et **Mot de passe** disparaissent, et le champ **ID d'informations d'identification** et le menu **Chambre forte de stockage des informations d'identification** apparaissent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans le menu **Chambre forte de stockage des informations d'identification** , sélectionnez Aucun, le coffre CyberArk ou un coffre de stockage des informations d'identification externe personnalisé.

> **Remarque :**
>
> Si le coffre-fort de CyberArk est sélectionné, le menu **Clé de recherche** s'affiche avec quatre choix de clé de recherche : ID d'informations d'identification, Adresse IP, FQDN, Tous les éléments ci-dessus. La sélection de Toutes les options ci-dessus peut dégrader les performances, car elle nécessite d'accéder au coffre-fort plusieurs fois.

a. Pour utiliser un coffre de stockage des informations d'identification externe personnalisé, accédez à Configurations du coffre-fort [vault_configuration.list] dans l'instance.

b. Créer un enregistrement à l'aide d'un nom associé à un fichier JAR importé pour un programme de résolution d'informations d'identification personnalisé.

Consultez les procédures Créer un fichier JAR pour résoudre les informations d'identification et Importer un fichier JAR pour résoudre les informations d'identification pour en savoir plus sur la création d'un coffre de stockage des informations d'identification externe personnalisé.

6. Remplissez le formulaire Informations d'identification en utilisant les champs de la table suivante.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
ID de certification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Il s'agit de l'ID transmis à la classe Java dans la carte des paramètres : `public static final String ARG_ID = "id";` Le Serveur MID utilise cet identificateur pour résoudre les informations d'identification réelles sur le référentiel. **Remarque :** Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Balise	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé.
Chambre forte de stockage des	Choisissez le coffre de stockage des informations d'identification externe dans la liste des coffres disponibles. Le menu est composé d'enregistrements

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
informations d'identification	de la section Configurations du coffre-fort [vault_configuration.list]. De nouveaux enregistrements peuvent être ajoutés et utiliser des noms associés aux fichiers JAR pour le programme de résolution des informations d'identification personnalisés. Consultez les procédures Créer un fichier JAR pour résoudre les informations d'identification et Importer un fichier JAR pour résoudre les informations d'identification pour en savoir plus sur la création d'un coffre de stockage des informations d'identification externe personnalisé.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Entrez l'ordre (séquence) dans lequel la plateforme teste ces informations d'identification lorsqu'elle tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des numéros élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), Discovery ou Orchestration essaie les informations d'identification aléatoirement.

7. Cliquez sur **Envoyer**.

Configurer l'identificateur d'informations d'identification pour AWS

Configurez votre instance pour obtenir les informations d'identification à partir d'un référentiel distant.

Avant de commencer

Rôle requis : cloud_admin

Vérifiez que ces modules d'extension sont actifs et que le Serveur MID a été installé :

- Discovery (com.snc.discovery)
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Stockage d'informations d'identification externe [com.snc.discovery.external_credentials]

Pourquoi et quand exécuter cette tâche

Ces procédures supposent que vous disposez déjà d'un référentiel externe configuré avec les informations d'identification que vous souhaitez protéger. L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé aux informations d'identification réelles dans le référentiel via le fichier JAR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Découverte** > **Informations d'identification**.
2. Sélectionnez les informations d'identification prises en charge par votre fournisseur de stockage d'informations d'identification externe.
3. Remplissez le formulaire en utilisant les champs de la table.

Champ	Description
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, Amazon Web Services.
Actif	Case à cocher pour activer ou désactiver les informations d'identification.
ID de certification	Saisissez le nom sous lequel ces informations d'identification sont stockées dans le fournisseur de stockage d'informations d'identification externe.
Serveurs MID	Sélectionnez un ou plusieurs serveurs MID qui peuvent utiliser ces informations d'identification.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque le stockage externe est activé, le champ **ID d'informations d'identification** s'affiche. Si cette case n'est pas visible, cliquez sur l'icône de menu dans la barre d'en-tête et sélectionnez **Vue** > **Stockage externe** dans le menu contextuel.
Chambre forte de stockage des informations d'identification	Sélectionnez **CyberArk**.

4. Cliquez sur **Envoyer**.

CyberArk Intégration de stockage des informations d'identification

L'intégration Serveur MIDCyberArk au coffre-fort permet ServiceNow® Orchestrationà , ServiceNow® Découverte et ServiceNow® Mappage des services de s'exécuter sans stocker d'informations d'identification sur l'instance.

Présentation de CyberArk

CyberArk Le produit Application Identity Management (AIM) utilise la solution de sécurité des comptes privilégiés pour éliminer la nécessité de stocker les mots de passe d'application intégrés dans des applications, des scripts ou des fichiers de configuration, et permet à ces mots de passe hautement sensibles d'être stockés, journalisés et gérés de manière centralisée dans le CyberArk coffre-fort. Cette approche permet aux organisations de se conformer aux exigences internes et réglementaires de remplacement périodique des mots de passe et de surveiller les activités associées à tous les types d'identités privilégiées, que ce soit sur site ou dans le cloud.

L'instance gère un identificateur unique pour chaque information d'identification, le type d'information d'identification (par exemple, SSH, SNMP ou Windows) et toutes les relations d'identification. Le obtient Serveur MID l'identificateur d'informations d'identification, le type d'informations d'identification et l'adresse IP de l'instance, puis utilise le CyberArk coffre pour résoudre ces éléments en informations d'identification utilisables. Le résolveur d'informations d'identification peut également rechercher le nom d'hôte, le nom de domaine complet et utiliser la recherche DNS inversée pour obtenir le nom de domaine complet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’intégration CyberArk nécessite le ServiceNow® module d’extension Stockage des informations d’identification externe, disponible dans **Définitions des systèmes** > **Modules d'extension**. Le Serveur MID client AIM/API doit CyberArk être installé sur le même ordinateur. Les versions 12.0.1 et ultérieures de CyberArk Application Access Manager (AAM) Credential Providers sont prises en charge.

Installé avec CyberArk

- **Règle métier** : la règle métier Stockage des informations d’identification externe effectue les tâches suivantes lorsqu’un administrateur apporte des modifications à la propriété de stockage des informations d’identification externe :
  - Elle remplace la vue de la liste et du formulaire d'enregistrement Informations d'identification par la vue Stockage externe. Cette vue permet aux utilisateurs d’afficher la colonne ID d’informations d’identification dans la liste.
  - Indique à l’d’actualiser son cache d’informations d’identification Serveur MID non externes en vue d’un changement dans la façon dont les informations d’identification sont obtenues.
- **Propriété système** : une propriété appelée Activer le stockage des informations d’identification externe [com.snc.use_external_credentials] active ou désactive le module d’extension Stockage des informations d’identification externe après son activation. Cette propriété est située à**Définition de découverte** > **Propriétés**et**Orchestration** > **Propriétés de serveur MID**et est activé lorsque vous activez le module d’extension.

> **Remarque :**
> Si vous désactivez le stockage des informations d’identification externes avec la propriété système, le système définit automatiquement toutes les informations d’identification externes comme inactives dans l’instance. Si vous réactivez la fonctionnalité avec cette propriété, le système ne réinitialise pas les enregistrements d’informations d’identification externes sur actif. Vous devez réactiver chaque enregistrement d’informations d’identification manuellement.

Types d’informations d’identification pris en charge

L’intégration CyberArk prend en charge ces ServiceNow types d’informations d’identification :

- GCP
- Azure
- CIM
- JMS
- Forum SNMP
- SNMPv3
- Authentification de base
- Paire de clés SSH
- Clé privée SSH (avec clé, phrase de passe et mot de passe)
- VMware
- Windows
- Informations d'identification applicatives

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour utiliser CyberArk l'intégration avec le type d'informations d'identification GCP, vous devez modifier le fichier jar de stockage des informations d'identification externe. Pour plus d'informations, consultez Outil de résolution des informations d'identification ServiceNow GCP à l'aide de CyberArk .

ServiceNow AI Platform Les fonctionnalités qui utilisent ces protocoles réseau prennent également en charge l'utilisation des informations d'identification stockées sur un CyberArk coffre-fort.

Informations d'identification prises en charge par le protocole réseau

Protocole réseau	ServiceNow® Studio de workflow soutien	Orchestration soutien
SOAP	Étape SOAP	Créer une activité de service Web SOAP avec des remplacements d'authentification de base
REST	Étape REST	Créer une activité de service Web REST avec des remplacements d'authentification de base
JDBC	Étape JDBC	Activité JDBC
SSH	Étape SSH	Activité SSH
PowerShell	Étape PowerShell	Activité PowerShell
SFTP	Étape SFTP	Activité SFTP
JMS		Activité JMS

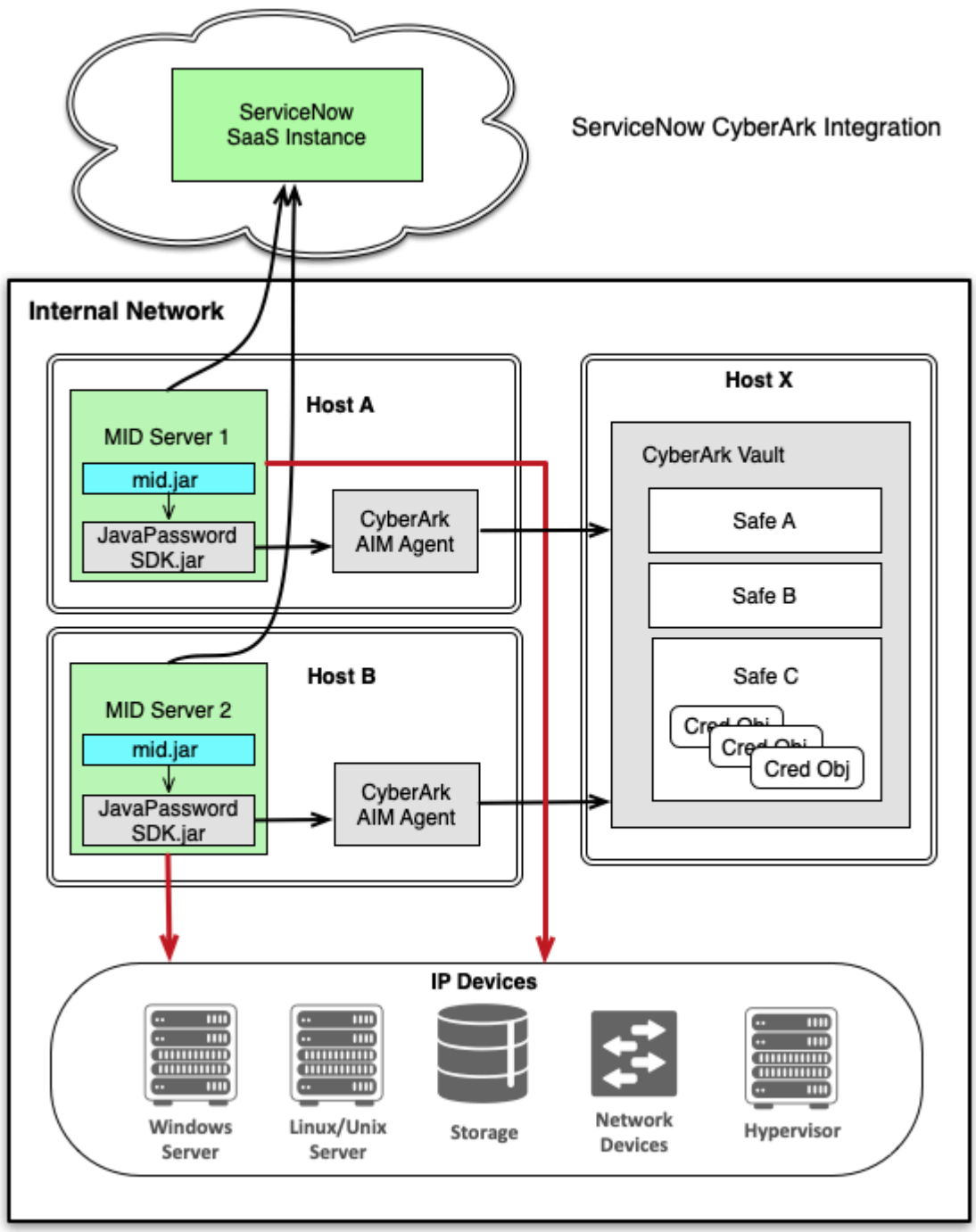
Important :
Vous ne pouvez pas gérer les informations d'identification stockées sur un CyberArk coffre et un système de stockage d'informations d'identification externe personnalisé à l'aide de cette même méthode Serveur MID. Le Serveur MID client AIM/API doit CyberArk être installé sur le même ordinateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture CyberArk

CyberArk Architecture de stockage



Remarque :
CyberArk Utilise le fichier `de mid.jar` du système de base pour résoudre les informations d'identification.

Comment le Serveur MID gère les Windows comptes

La recherche d'informations d'identification tente initialement de faire correspondre l'ID d'informations d'identification spécifié à une valeur existante dans le champ **Nom**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

du CyberArk coffre. Si une correspondance est trouvée, ces informations d'identification sont renvoyées. Si aucune correspondance n'est trouvée, la recherche d'informations d'identification tente de trouver une correspondance à l'aide de l'adresse IP. Si la recherche d'adresse IP correspond à plusieurs informations d'identification, telles que Windows et Tomcat sur le même serveur, la recherche échoue. Pour éviter ce problème, définissez le *ext.cred.type_specifier* paramètre dans le Serveur MID fichier config.xml sur **true** pour forcer CyberArk le renvoi d'informations d'identification qui correspondent à la fois au type d'informations d'identification et à l'adresse IP. Par exemple, si une adresse IP est partagée par les deux Windows et , Tomcat un type d'information d'identification renvoie Windows uniquement les informations d'identification Windows .

Mettre à niveau la CyberArk bibliothèque

Vous pouvez mettre à niveau la CyberArk bibliothèque si un paramètre de configuration sécurisé est nécessaire.

Vérifiez le paramètre de configuration suivant dans le **config.xml** : <nom du paramètre="mid.secure_config.provider » value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider"/>

Procédez comme suit pour effectuer la mise à niveau si un fournisseur de paramètres de configuration sécurisé est configuré.

1. Renommez la CyberArk version du client en JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar.
2. Créez une nouvelle entrée jar dans la table ecc_agent où le fichier jar renommé peut être joint. Cette nouvelle entrée est téléchargée dans le fichier Serveur MID. Cette étape génère deux fichiers jar (Passworsdk.jar et JavaPasswordSDK _12_X_X.jar).
3. Supprimez l'ancienne entrée de ecc_agent de l'instance. Cette étape supprime Passworsdk.jar de , Serveur MID et le _12_X_X.jar JavaPasswordSDK reste dans le système.

Configuration de l'intégration de CyberArk

Ces procédures comprennent à la fois des tâches de configuration de CyberArk et de ServiceNow, y compris des références à la documentation appropriée de CyberArk.

L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé au nom des informations d'identification dans le coffre-fort de CyberArk. Lors de la recherche d'informations d'identification, le serveur MID trouve les informations d'identification en faisant correspondre l'identificateur d'informations d'identification à un nom dans le coffre-fort, qui doit être unique. Si l'identificateur d'informations d'identification est vide, le serveur MID trouve les informations d'identification par adresse IP. Pour identifier les informations d'identification par adresse IP, le système examine le type d'informations d'identification pour s'assurer qu'il n'existe qu'une seule information d'identification de ce type à cette adresse. Par exemple, lorsqu'un serveur Windows et vCenter s'exécutent tous deux sur la même adresse IP. Pour prendre en charge des exigences strictes en matière d'informations d'identification comme celle-ci dans un environnement SSH, un paramètre de configuration de MID Server vous permet d'exiger que le type d'informations d'identification demandé corresponde au type renvoyé par CyberArk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le champ **ID d'informations d'identification** est le seul champ nécessaire pour mapper vos informations d'identification à CyberArk, dans tous les cas à l'exception de SNMPv3. Le champ **ID d'informations d'identification de confidentialité** est facultatif et requis uniquement lors de l'utilisation des informations d'identification SNMPv3 et d'un protocole de confidentialité pour les informations d'identification. Reportez-vous à la rubrique Configurer l'identificateur d'informations d'identification CyberArk pour en savoir plus.

Pour configurer votre instance afin d'obtenir les informations d'identification d'un coffre-fort CyberArk, effectuez ces tâches dans l'ordre dans lequel elles apparaissent ci-dessous.

Configurer le coffre-fort CyberArk et installer l'API AIM

Configurez le coffre-fort CyberArk pour permettre l'accès au serveur MID et installez l'API CyberArk AIM sur la machine du serveur MID.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, assurez-vous que le module d'extension Stockage des informations d'identification externe est activé. Les versions 12.0.1 et ultérieures de CyberArk Application Access Manager (AAM) Credential Providers sont prises en charge.

Procédure

1. Configurez le coffre-fort CyberArk avec l'ID de l'application et les détails d'authentification que tous les serveurs MID demandant des informations d'identification utiliseront.
   Pour plus d'informations, reportez-vous au fournisseur d'informations d'identification CyberArk et au guide de mise en œuvre de l'ASCP.

   a. Assurez-vous que CyberArk est configuré pour permettre au serveur MID d'accéder au coffre-fort en créant un ID d'application dans CyberArk appelé `ServiceNow_MID_Server`.

   b. Assurez-vous que chaque identifiant de connexion dont le serveur MID a besoin a accès à l'ID d'application `ServiceNow_MID_Server` .

   Remarque :
   Vous pouvez remplacer le **ServiceNow_MID_Server** App-ID par défaut dans le fichier de config.xml du serveur MID à l'aide du paramètre ext.cred.app_id . Si vous modifiez la valeur de ce paramètre, assurez-vous de configurer une valeur correspondante dans le coffre.

2. Installez le fournisseur d'informations d'identification CyberArk, y compris l'API AIM, sur chaque ordinateur qui héberge un service de serveur MID utilisé pour accéder à la banque d'informations d'identification.
3. Mettez en service les comptes CyberArk et définissez les autorisations d'accès aux applications.
   Pour plus d'informations, reportez-vous au Guide de mise en œuvre de la sécurité des comptes privilégiés de CyberArk.

   a. Dans le coffre-fort CyberArk Password Safe, créez les comptes privilégiés requis par Découverte, Orchestration ou Service Mapping pour accéder à différents appareils et assurez-vous que ces comptes sont membres des coffres-forts dans lesquels les informations d'identification nécessaires sont stockées.

   b. Ajoutez le fournisseur d'informations d'identification et les utilisateurs de l'application en tant que membres des coffres de mots de passe où sont stockés les mots de passe des applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer le fichier JAR de CyberArk

Importez le fichier CyberArk JavaPasswordSDK.jar dans l'instance pour le rendre accessible au serveur MID.

Avant de commencer

Rôle requis : agent_admin ou admin

Avant de commencer cette procédure, assurez-vous que CyberArk est configuré pour permettre au serveur MID d'accéder aux informations d'identification. Assurez-vous que l'API CyberArk AIM est installée sur chaque serveur hébergeant un serveur MID utilisé pour accéder au coffre-fort.

Remarque :
Deux intégrations CyberArk distinctes ne sont pas prises en charge par le MID Server. La même version de l'API CyberArk AIM doit être installée sur tous les serveurs MID connectés à la même instance.

Pourquoi et quand exécuter cette tâche

Utilisez ce processus même si le fichier JavaPasswordSDK.jar existe déjà sur le serveur MID.

Procédure

1. Accédez à la **Tous** > **Serveur MID** > **Fichiers JAR**.
2. Cliquez sur **Nouveau**.
3. Remplissez le formulaire à l'aide des champs de la table.

Champs du formulaire Fichier JAR

Champ	Description
Nom	Nom unique et descriptif permettant d'identifier le fichier dans l'instance.
Version	Numéro de version facultatif du fichier, s'il est disponible.
Source	Fournisseur du fichier JAR. Les informations sources ne sont pas utilisées par le système.
Description	Brève description facultative du fichier JAR et de son objectif dans l'instance.

4. Joignez le fichier JAR à cet enregistrement.
   Le fichier AIM JavaPasswordSDK.jar est fourni avec les fichiers d'installation du SDK AIM et se trouve généralement sur le serveur MID dans le répertoire d'installation AIM à l'adresse <install_dir>/CyberArk/ApplicationPasswordSdk.

   Remarque :
   Le JavaPasswordSDK.jar AIM joint doit correspondre à la version installée de l'API AIM de CyberArk. Toute incompatibilité dans JavaPasswordSDK.jar fichiers peut entraîner un comportement imprévisible et des problèmes de fonctionnalité potentiels.

5. Cliquez sur **Envoyer**.
6. Redémarrez le service Serveur MID.
   La plateforme met le fichier JAR à la disposition de tout serveur MID configuré pour communiquer avec l'instance.

Configurer le Serveur MID pour CyberArk

Configurez le fichier config.xml pour accorder au serveur MID l'accès au coffre-fort CyberArk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, importez le fichier JavaPasswordSDK.jar dans l'instance.

Procédure

Configurer manuellement Serveur MID Ajoutez un fichier de paramètres de Serveur MID avec ces paramètres.

Cette configuration ne peut pas être effectuée à partir de l'instance.

Paramètres de configuration requis

Paramètre	Valeur	Description
ext.cred.safe_folder	NameOfFolder	Dossier à utiliser pour toutes les recherches d'informations d'identification. Par exemple, **root**.
ext.cred.use_cyberark	vrai	Paramètre booléen indiquant que ce serveur MID est intégré à CyberArk.

Paramètres de configuration facultatifs

Paramètre	Valeur	Description
ext.cred.safe_timeout	5 (secondes)	Délai d'expiration de chaque recherche d'informations d'identification dans le coffre-fort, spécifié en secondes.
ext.cred.safe_name	NameOfSafe	Nom sécurisé par défaut utilisé pour toutes les recherches d'informations d'identification. Si les paramètres se trouvent dans plusieurs coffres-forts, l'identifiant de connexion peut être spécifié au format *<safeName>:<CredentialID>*. Lorsqu'il est configuré de cette manière, le champ **NameOfSafe** est ignoré. Si tous les identifiants externes sont spécifiés dans ce format, omettez le champ **NameOfSafe** . **Remarque :** Par défaut, le caractère de séparation dans ce format est un deux-points. Pour attribuer un caractère à votre choix comme séparateur, ajoutez cette ligne au fichier CredMap.properties : safe.cred.split.string=<string>.
ext.cred.app_id	ServiceNow_MID_Server	Spécifie l'ID d'application utilisé pour accorder au serveur MID l'autorisation d'accéder au coffre-fort CyberArk. La valeur par défaut, **ServiceNow_MID_Server**, doit être définie dans le coffre-fort de CyberArk. Vous pouvez utiliser ce paramètre pour remplacer la valeur par défaut et spécifier votre propre ID d'application. Si vous modifiez l'ID de l'application dans ce paramètre, assurez-vous de configurer CyberArk pour qu'il corresponde.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Valeur	Description
ext.cred.type_specifier	vrai	Force une recherche d'adresse IP pour renvoyer des informations d'identification qui correspondent à la fois à l'ID de la plateforme CyberArk et à l'adresse IP. Par exemple, si une adresse IP est partagée par Windows et Tomcat, une information d'identification avec un ID de plateforme commençant par **Win** renvoie uniquement les informations d'identification Windows. Lorsque ce paramètre est défini sur vrai, CyberArk recherche les ID de plateforme qui commencent par : • Win : Windows • Unix : SSH • VMware : VMware
ext.cred.check_ssh_type	Faux	Lorsque la valeur est définie sur vrai, le type d'informations d'identification SSH renvoyées par CyberArk doit correspondre au type d'informations d'identification demandées. Par exemple, si un nom d'utilisateur/mot de passe SSH normal est demandé et que seules les clés SSH sont disponibles, la recherche d'informations d'identification échoue.

Configurer les informations d'identification CyberArk for SNMPv2

Si votre système utilise SNMPv2, vous pouvez créer un fichier spécial pour mapper l'attribut d'une information d'identification à la chaîne de communauté.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, configurez le serveur MID pour avoir accès au coffre-fort CyberArk.

Pourquoi et quand exécuter cette tâche

Remarque :
Si la chaîne de communauté apparaît dans le champ de mot de passe des informations d'identification CyberArk, il n'est pas nécessaire d'effectuer cette procédure.

SNMPv2 n'est pas pris en charge nativement dans CyberArk. Si votre organisation a créé des informations d'identification SNMPv2 personnalisées dans lesquelles la chaîne de communauté n'apparaît pas dans le champ de mot de passe des informations d'identification, utilisez cette procédure pour mapper l'attribut des informations d'identification à la chaîne de communauté.

Procédure

1. Dans un éditeur de texte, créez un fichier appelé CredMap.properties, contenant ce code : `SNMPv2.Communauté=attribute_name`
2. Enregistrez le fichier dans le répertoire /agent de votre installation de Serveur MID.
   Lors de la recherche d'informations d'identification, le Serveur MID tente de trouver cet attribut pour les informations d'identification. Si l'attribut est introuvable, le serveur MID recherche alors dans le champ de mot de passe. Si le champ Mot de passe est vide, la recherche d'informations d'identification échoue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'identificateur d'informations d'identification CyberArk

Créez la clé unique que CyberArk peut utiliser pour identifier des informations d'identification spécifiques dans le référentiel externe.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, assurez-vous que le module d'extension Stockage des informations d'identification externe est activé et que la propriété système com.snc.use_external_credentials est définie sur true.

Procédure

1. Accédez à la **Tous** > **Découverte** > **Informations d'identification** ou **Orchestration** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Dans la liste des types d'informations d'identification, sélectionnez un type qui prend en charge le stockage externe CyberArk.
4. Remplissez le formulaire à l'aide des champs de votre type d'informations d'identification.
5. Sélectionnez la case à cocher **Banque d'identifiants externes** .
   Les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID des informations d'identification** .

   Remarque :
   Si la case n'est pas visible, cliquez sur l'icône de menu dans la barre d'en-tête et sélectionnez **Vue** > **Stockage externe**.

6. Dans le champ **ID d'informations d'identification** , saisissez une expression à l'aide de l'un des formats suivants :
   - Si toutes vos informations d'identification se trouvent dans le même coffre-fort, configurez ce nom de coffre-fort dans le fichier de config.xml Serveur MID à l'aide du paramètre ext.cred.safe_name , puis spécifiez l'ID d'informations d'identification par son nom uniquement, en tant qu **<ID d'informations d'identification>**.
   - Pour nommer les informations d'identification d'une plateforme donnée qui résident dans un SAFe spécifique, définissez l'ID d'informations d'identification **comme < sécurisé > :<ID d'informations d'identification > :<ID de la plateforme>**.
   - Si vos informations d'identification se trouvent dans plusieurs coffres-forts, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :<ID d'informations d'identification>**.
   - Si vous souhaitez que CyberArk recherche les informations d'identification par adresse IP, à l'aide d'un autre coffre-fort, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :**.
   - Si vous souhaitez que CyberArk recherche les informations d'identification d'un autre ID de plateforme dans le même coffre-fort, utilisez le format suivant : **::<ID de la plateforme>**
   - Si vous souhaitez que CyberArk recherche les informations d'identification dans un coffre-fort configuré par l'adresse IP plutôt que par l'ID d'informations d'identification, laissez ce champ vide. Il s'agit de la meilleure pratique pour gérer les installations dans lesquelles chaque serveur possède des informations d'identification uniques. Sans ce type de recherche, vous devez créer un enregistrement d'ID d'informations d'identification dans votre instance pour chaque serveur de votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
L'ID d'informations d'identification doit correspondre à la valeur du champ **Nom** du compte CyberArk. Le champ **ID d'informations d'identification** a une limite de 180 caractères.

7. Si vous stockez des informations d'identification SNMPv3 dans CyberArk et que vous utilisez le protocole de confidentialité et la clé de confidentialité, configurez l'ID comme suit :

   a. Dans le champ **Type de banque d'identifiants** , sélectionnez **CyberArk**.
   Le champ **ID d'informations d'identification de confidentialité** s'affiche.

   b. Saisissez le **nom** du compte de confidentialité CyberArk SNMPv3 dans le champ **ID d'informations d'identification de confidentialité** .

8. Cliquez sur **Envoyer**.

Configurer les informations d'identification AWS sur un coffre-fort CyberArk

Configurez votre coffre-fort CyberArk avec les informations d'identification AWS à récupérer pour être utilisées par votre instance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Stockez les informations d'identification en tant que compte sur le coffre-fort CyberArk. Lorsque vous configurez l'accès au coffre sur votre instance, le nom que vous donnez au compte doit également être utilisé comme ID d'informations d'identification.

Remarque :
La procédure qui suit fait référence à CyberArk Password Vault v14.2.1. Si vous utilisez une version différente, configurez la configuration conformément à la documentation officielle de CyberArk Password Vault.

Procédure

1. Dans CyberArk, accédez à **Comptes** > **Comptes et demandes** > **Vue des comptes** > **Ajouter un compte**.
2. Sélectionnez le type de système : **Service dans le cloud**.
3. Affecter à la plateforme : **Amazon Web Services - AWS - Clés d'accès**.
4. Stocker dans un coffre-fort : sélectionnez un coffre-fort dans la liste.
5. Définir les propriétés : Entrez les informations suivantes :

Informations d'identification CyberArk

Champ	Valeur
Nom d'utilisateur AWS IAM	Saisissez la clé d'accès AWS fournie par AWS.
Secret de clé d'accès AWS (facultatif)	Saisissez la clé d'accès secrète AWS fournie par AWS.
Personnaliser le nom du compte	Activez/désactivez le curseur pour entrer un nom personnalisé pour cette clé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
ID de clé d'accès AWS	Saisissez à nouveau la clé d'accès AWS fournie par AWS.
Numéro d'ID de compte AWS	Saisissez à nouveau la clé d'accès AWS fournie par AWS.
Nom de l'alias du compte AWS (facultatif)	Saisissez un nom d'alias pour le compte.

6. Choisissez **Ajouter**.

Que faire ensuite

Si vous ne l'avez pas déjà fait, créez un identificateur d'informations d'identification sur votre instance pour configurer l'accès au coffre-fort CyberArk. Pour plus d'informations, consultez Configurer l'accès au stockage d'informations d'identification externe pour AWS.

Configurer les informations d'identification AWS dans un coffre-fort CyberArk à l'aide de l'interface utilisateur classique

Configurez votre coffre-fort CyberArk avec les informations d'identification AWS à récupérer pour être utilisées par votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

CyberArk Password Vault v14.2.1 inclut des options de configuration Vue des comptes et Vue des comptes (interface utilisateur classique) pour stocker les informations d'identification en tant que compte. Lorsque vous configurez l'accès au coffre sur votre instance, le nom que vous donnez au compte doit également être utilisé comme ID d'informations d'identification.

Remarque :
La procédure qui suit fait référence à CyberArk Password Vault v14.2.1. Si vous utilisez une version différente, configurez la configuration conformément à la documentation officielle de CyberArk Password Vault.

Procédure

1. Dans CyberArk, accédez à **Comptes** > **Comptes et demandes** > **Vue des comptes (interface utilisateur classique)** > **Ajouter un compte**.
2. Saisissez les informations suivantes :

Informations d'identification CyberArk

Champ	Valeur
Type d'équipement	Sélectionnez **Service dans le cloud**.
Nom de la plateforme	Sélectionnez **Amazon Web Services : AWS : clés d'accès**.
Nom d'utilisateur AWS IAM	Saisissez la clé d'accès AWS fournie par AWS.
ID de clé d'accès AWS	Saisissez à nouveau la clé d'accès AWS fournie par AWS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Numéro d’ID de compte AWS	Saisissez à nouveau la clé d’accès AWS fournie par AWS.
Secret de clé d’accès AWS	Saisissez la clé d’accès secrète AWS fournie par AWS.
Nom	Entrez un nom personnalisé pour cette clé.

3. Choisissez **Enregistrer**.

Que faire ensuite

Si vous ne l’avez pas déjà fait, créez un identificateur d’informations d’identification sur votre instance pour configurer l’accès au coffre-fort CyberArk. Pour plus d’informations, consultez Configurer l’accès au stockage d’informations d’identification externe pour AWS.

Configurer les informations d’identification Azure sur un coffre-fort CyberArk

Configurez votre coffre-fort CyberArk avec les informations d’identification Azure à récupérer pour être utilisées par votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Pour stocker des informations d’identification Azure, créez d’abord un modèle d’informations d’identification Azure dans le coffre-fort CyberArk. Ce processus ne doit être effectué qu’une seule fois pour le coffre-fort.

Procédure

1. Connectez-vous à CyberArk en mode Administration.
2. Accédez à l’onglet **Administration** .
3. Dans **Configuration du système**, modifiez **Gestion de la plateforme**.
4. Accédez au **modèle du fournisseur** dans le cloud et dupliquez-le.
5. Modifiez le modèle pour les informations d’identification Azure.
6. Ajoutez les deux propriétés suivantes :
   - *Name*au fur et à *Display Name* mesure *UsernameClient ID*
   - *Name*au fur et à *DisplayName* mesure *AddressTenant ID*
7. Appliquer les changements.
8. Accédez à la section **Compte** , puis sélectionnez **Ajouter un compte**.
9. Sélectionnez **Sûr**.
10. Définissez le **type d’appareil** sur **Service dans le cloud**.
11. Sélectionnez le modèle Azure qui a été modifié précédemment.
12. Renseignez les informations pour les champs **ID client**, **ID de locataire** et **Mot de passe** .
13. Sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification OAuth 2.0 via Serveur MID le stockage d'informations d'identification externe

Stockez les informations d'identification OAuth 2.0 (ID client et secret client) dans le CyberArk coffre-fort au lieu de l'instance ServiceNow . Obtient Serveur MID les informations d'identification CyberArk du coffre, si nécessaire pour obtenir le jeton OAuth. Le jeton est stocké dans le serveur MID et actualisé automatiquement à son expiration.

Le CyberArk produit Application Identity Management (AIM) utilise la solution de sécurité des comptes privilégiés pour éliminer la nécessité de stocker les mots de passe d'application intégrés dans des applications, des scripts ou des fichiers de configuration, et permet de stocker, de consigner et de gérer ces mots de passe hautement sensibles de manière centralisée dans le CyberArk coffre-fort. Vous pouvez configurer le coffre pour stocker les informations d'identification OAuth 2.0 plutôt que directement dans un enregistrement d'informations CyberArkServiceNow d'identification. Pour en savoir plus sur CyberArk, consultez CyberArk Intégration de stockage des informations d'identification.

Architecture de l'authentification OAuth 2.0 de la Serveur MID demande

L'architecture comporte deux parties : ServiceNow l'instance et l'environnement dans lequel le client Application Identity Manager (AIM) et le serveur MID sont configurés. Le cloud ou un environnement client sont des exemples d'environnement.

Le Serveur MID client et Application Identity Manager (AIM) doivent être configurés sur le même environnement et Application Identity Manager (AIM) doit être configuré pour interagir avec le coffre-fort CyberArk externe. Le CyberArk coffre-fort externe peut être hébergé dans le même environnement que celui de MID Server et d'Application Identity Manager (AIM) ou dans un environnement différent.

L'instance ServiceNow gère les identificateurs d'informations d'identification qui correspondent à des informations d'identification OAuth 2.0 spécifiques stockées dans le CyberArk coffre. Avant d'envoyer une demande de jeton OAuth, le serveur MID obtient l'identificateur d'informations d'identification de l'instance, puis utilise un fichier JAR fourni par le client pour envoyer l'identificateur au client AIM. Le client AIM envoie la demande au CyberArk coffre. Le CyberArk coffre renvoie les informations d'identification OAuth 2.0 au serveur MID via le client AIM. Après avoir reçu les informations d'identification OAuth 2.0, le serveur MID envoie la demande de jeton OAuth au serveur d'autorisation tiers. La demande de jeton comprend des informations telles que le client et le secret client qu'elle CyberArk stocke, le périmètre OAuth et l'URL du jeton que l'instance stocke. Une fois que le serveur d'autorisation a émis le jeton OAuth, le serveur MID le stocke dans sa mémoire cache.

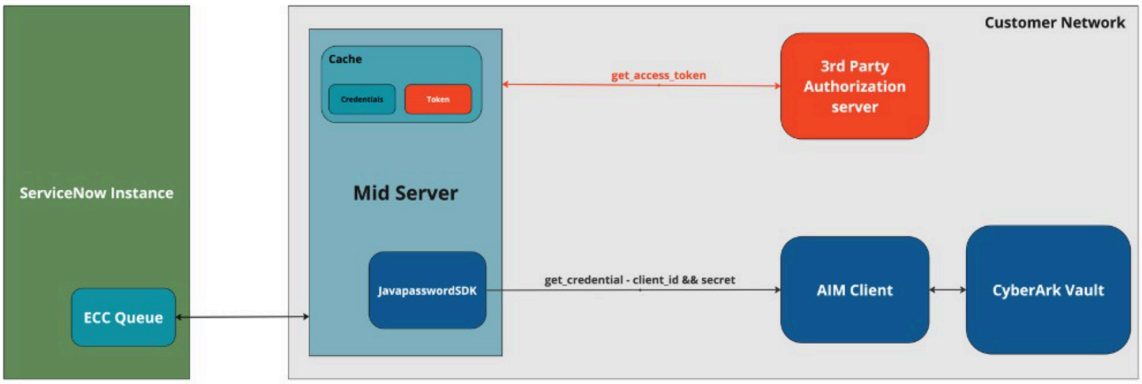
Remarque :
Cette fonctionnalité prend en charge le type d'accord Informations d'identification du client.

L'image montre le processus d'authentification de demande du Serveur MID.

Remarque :
Il est supposé que le serveur d'autorisation tiers et le CyberArk coffre-fort sont hébergés dans le réseau du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer un fichier JAR et des identificateurs d'identification

Configurez un fichier JAR et des identificateurs d'identification de sorte que le fichier JAR résolve les identificateurs d'informations d'identification en informations d'identification réelles du CyberArk coffre-fort externe. Ce processus permet au serveur MID d'obtenir et d'inclure les informations d'identification OAuth 2.0 dans la demande de jeton OAuth.

Avant de commencer

Rôle requis : agent_admin ou admin

Le CyberArk coffre-fort externe stocke les informations d'identification sensibles et l'instance ServiceNow stocke les identificateurs d'informations d'identification qui correspondent aux noms d'informations d'identification spécifiques que le coffre-fort stocke. Le fichier JAR permet le mappage d'un identificateur d'informations d'identification à un nom d'information d'identification spécifique dans le coffre-fort externe. Le mappage permet d'acquérir et d'inclure Serveur MID les informations d'identification requises dans la demande de jeton OAuth. Vous devez configurer les identificateurs d'identification et le fichier JAR respectivement dans l'instance ServiceNow et le serveur MID.

Procédure

1. Importer le fichier JAR de CyberArk.
2. Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe.

Configurer CyberArk

Configurez le coffre-fort pour stocker les CyberArk informations d'identification OAuth 2.0 et répondre aux demandes d'informations d'identification OAuth 2.0 à partir Serveur MID du .

Avant de commencer

Confirmez que vous êtes abonné au programme d'installation du pack standard de Centre d'intégration ServiceNow. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Rôle requis : agent_admin ou admin

Procédure

1. Configurer le coffre-fort CyberArk et installer l'API AIM.
2. Importer le fichier JAR de CyberArk.
3. Configurer les informations d'identification OAuth 2.0 sur CyberArk.
4. Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les informations d'identification OAuth 2.0 sur CyberArk

Configurez votre coffre-fort CyberArk avec les informations d'identification OAuth 2.0 demandées par l'instance ServiceNow .

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Pour stocker les informations d'identification OAuth 2.0, créez d'abord un modèle d'informations d'identification OAuth 2.0 dans le coffre-fort CyberArk. Ce processus ne doit être effectué qu'une seule fois pour le coffre-fort.

Procédure

1. Procédez comme suit si vous configurez les informations d'identification OAuth 2.0 pour la première fois.

   a. Connectez-vous à CyberArk en mode Administration.

   b. Accédez à l'onglet **Administration** .

   c. Sélectionnez **Gestion de la plateforme**.
   La page Gestion des plateformes affiche les plateformes sous l'onglet Cibles.

   d. Développez un type de plateforme.

   e. Sélectionnez l'icône des paramètres () qui correspond à un modèle de plateforme et sélectionnez **Dupliquer**.

   f. Dans la fenêtre Dupliquer la plateforme, donnez un nom au modèle et sélectionnez **Créer**.

   Remarque :
   Notez le type de système sous lequel vous avez créé un modèle en double. Par exemple, Cloud Service est un type de système.

   g. Sélectionnez l'icône des paramètres (icône Paramètres de la ) qui correspond au modèle de plateforme en double que vous avez créé, puis sélectionnez **Modifier**.

   h. Ajoutez la propriété.
   Nom en tant que nom d'utilisateur et nom d'affichage en tant qu'ID client.

   i. Renommez les autres propriétés.

   Conseil :
   Choisissez des noms de propriétés pertinents pour OAuth 2.0.

   j. Sélectionnez **Appliquer**.
   Les mises à jour sont appliquées.

   k. Sélectionnez **OK**.

   l. Sur le panneau de gauche, accédez à Comptes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

m. Sélectionnez **Ajouter un compte**.

n. Sous l'en-tête Type de système, sélectionnez le type de système sous lequel vous avez créé le modèle de plateforme.
Le type de système affiche les modèles de plateforme.

o. Sous l'en-tête Sélectionner une plateforme, sélectionnez le modèle de plateforme que vous avez créé.

p. Sélectionnez Sûr.
Enregistrez la valeur Safe pour une utilisation ultérieure.

q. Renseignez les informations pour l'ID client, le mot de passe (indiquez le secret client comme valeur) et d'autres champs selon vos besoins.

r. Sélectionnez **Ajouter**.
Le compte est ajouté.

s. Sur la page Vue du compte, ouvrez un compte.

t. Sélectionnez l'onglet **Détails**.

u. Copiez la valeur stockée sous la section Nom du compte et enregistrez-la pour une utilisation ultérieure.
La valeur que vous avez copiée et stockée est utilisée comme identificateur d'informations d'identification dans l'instance ServiceNow.

2. Procédez comme suit si vous ne configurez pas les informations d'identification OAuth 2.0 pour la première fois.

a. Connectez-vous à CyberArk en mode Administration.

b. Accédez à la section **Compte** , puis sélectionnez **Ajouter un compte**.

c. Sélectionnez le type de système dans Type de **système** sous lequel se trouve le modèle de stockage d'OAuth 2.0.

d. Sélectionnez le modèle de plateforme requis que vous avez créé et sélectionnez **Sûr**.
Enregistrez la valeur Safe pour une utilisation ultérieure.

e. Renseignez les informations pour l'ID client, le mot de passe (indiquez le secret client comme valeur) et d'autres champs selon vos besoins.

f. Sélectionnez **Ajouter**.
Le compte est ajouté.

g. Sur la page Vue du compte, ouvrez un compte.

h. Sélectionnez l'onglet **Détails**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Copiez la valeur stockée sous la section Nom du compte et enregistrez-la pour une utilisation ultérieure. La valeur que vous avez copiée et stockée est utilisée comme identificateur d'informations d'identification dans l'instance ServiceNow .

Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe

Configurez une connexion pour envoyer des demandes de jetons OAuth 2.0 à un serveur d'authentification tiers via le Serveur MID. Ajoute Serveur MID les informations d'identification OAuth 2.0 (ID client et Secret client) du coffre-fort externe, du CyberArk périmètre OAuth et de l'URL de jeton de l'instance à la demande et les envoie au serveur d'authentification tiers.

Avant de commencer

Vérifiez les éléments suivants.

- Confirmez que vous êtes abonné au programme d'installation du pack standard de Centre d'intégration ServiceNow. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .
- Vous avez créé un fichier JAR qui permet au serveur MID de résoudre les informations d'identification avec le CyberArk coffre-fort externe. Consultez Créer un fichier JAR pour résoudre les informations d'identification.
- Vous avez importé le fichier JAR dans Serveur MID.
- Le MID Server est configuré pour CyberArk. Consultez Configurer le Serveur MID pour CyberArk.
- OAuth 2.0 est configuré sur le stockage externe de CyberArk. Consultez Configurer les informations d'identification OAuth 2.0 sur CyberArk.

Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer la connexion et les informations d'identification à l'aide d'un modèle de configuration ou manuellement. Un modèle de configuration définit les composants du formulaire d'enregistrement de connexion et est réutilisable pour les autres enregistrements de connexion. Manuellement, vous ne pouvez configurer la connexion qu'à cette fin. Le sujet montre les deux approches.

Procédure

1. Configurez la connexion à l'aide d'un modèle de configuration.

   a. Accédez à la **Tous** > **Centre d'intégration** > **Modèles de configuration**.

   b. Sélectionnez **Nouveau**.

   c. Sélectionnez **Connexion HTTP avec le type d'attribution Informations d'identification du client OAuth (Stockage externe).**

   d. Mettez à jour le formulaire, au besoin.
   Par exemple, vous pouvez fournir le champ d'application dans les champs `oauth_entity_profile_scope` et `oauth_entity_scope` de la section Modèle de données par défaut. Pour apprendre à créer un modèle de configuration, reportez-vous à la section Créer un modèle de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Sélectionnez **Soumettre**.
Vous avez créé le modèle de configuration.

f. Accédez à la **Tous** > **Centre d'intégration** > **Alias de connexion et d'informations d'identification**.

g. Mettez à jour le formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise de l'enregistrement d'informations d'identification migre vers un alias de connexion et d'informations d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas changé le nom pour respecter les restrictions de nommage.
Application	Identificateur unique pour l'alias de connexions et d'informations d'identification, basé sur le format `scope_name.alias_name`. ▪ Si le périmètre est global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ▪ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Alias parent	Option permettant de sélectionner l'alias sous lequel vous créez cet alias de connexion et d'informations d'identification. L'alias de connexion et d'informations d'identification que vous créez est un alias enfant. Un alias enfant est répertorié sous l'onglet **Alias enfants** sur la page de l'alias de connexion et d'informations d'identification parent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	
Type	Option pour indiquer le type d'alias que vous créez. Choisissez parmi les options suivantes. ▪ Informations d'identification : alias qui contient un enregistrement d'informations d'identification. ▪ Connexion et informations d'identification : alias qui contient à la fois l'enregistrement de connexion et d'informations d'identification. Cette option est sélectionnée par défaut. Confirmez que la connexion et les informations d'identification sont sélectionnées.
Prendre en charge plusieurs connexions actives	Désignateur indiquant si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et associez-les à l'alias à l'aide de la liste connexe Connexions.
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez Politique des nouveaux essais .
Modèle de configuration	Option permettant de sélectionner le modèle de configuration à partir duquel vous créez l'alias de connexion et d'informations d'identification. Sélectionnez le modèle du type **Connexion HTTP avec type d'attribution Informations d'identification du client OAuth (Stockage externe)** que vous avez créé.

h. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement d'alias de connexion et d'informations d'identification.

i. Accédez à la **Tous** > **Centre d'intégration** > **Tableau de bord des connexions**.

j. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement d'alias de connexion et d'informations d'identification que vous avez créé.

k. Sur l'enregistrement de l'alias de connexion et d'informations d'identification, sélectionnez **Afficher les détails**.

l. Sélectionnez **Configurer**.

m. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Configurer la connexion

Champ	Description
Nom de la connexion	Nom de la connexion. Vous ne pouvez pas mettre à jour le nom.
URL de connexion	URL du serveur tiers.
Utiliser MID	Option permettant d'activer Serveur MID. **Important :** Confirmez que l'option est sélectionnée.
Sélection de MID	Option permettant de spécifier la configuration MID pour la connexion. ▪ **Serveur MID spécifique** : option permettant d'indiquer une sélection manuelle d'un serveur MID spécifique. ▪ **Sélectionner automatiquement Serveur MID** : option permettant d'indiquer que vous souhaitez que le Serveur MID soit sélectionné automatiquement. ▪ **Grappe MID spécifique** : option permettant d'indiquer une sélection manuelle d'une grappe MID de serveurs MID. **Important :** Vérifiez que le serveur MID que vous sélectionnez réside sur la même machine que le client CyberArk AIM configuré pour accéder au coffre-fort CyberArk. Consultez Configurer le coffre-fort CyberArk et installer l'API AIM.
Serveur MID	Option permettant de spécifier manuellement un serveur MID. Cette option s'affiche si vous sélectionnez **Serveur MID spécifique** dans le champ **Sélection MID** .
Grappe MID	Option permettant de spécifier manuellement une grappe MID. Cette option s'affiche si vous sélectionnez **Grappe MID spécifique** dans le champ **Sélection MID** .
Banque d'informations d'identification externes	Option permettant d'utiliser le stockage d'informations d'identification externe CyberArk. Lorsque vous sélectionnez l'option, le serveur MID obtient les informations d'identification OAuth 2.0 (ID client et secret client) à partir du stockage d'informations d'identification externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Important : Confirmez que l'option est sélectionnée.
ID de certification	Identificateur du compte CyberArk qui détient les détails de l'ID client et du secret client. Pour afficher la procédure d'obtention de l'identificateur d'identification, reportez-vous à la section Configurer les informations d'identification OAuth 2.0 sur CyberArk. Dans le champ ID d'informations d'identification, saisissez une expression à l'aide de l'un de ces formats. ▪ Si toutes vos informations d'identification se trouvent dans le même coffre-fort, configurez ce nom de coffre-fort dans le fichier de config.xml Serveur MID à l'aide du paramètre ext.cred.safe_name , puis spécifiez l'ID d'informations d'identification par son nom uniquement, en tant qu **<ID d'informations d'identification>**. ▪ Pour nommer les informations d'identification d'une plateforme donnée qui résident dans un SAFe spécifique, définissez l'ID d'informations d'identification **comme < sécurisé > :<ID d'informations d'identification > :<ID de la plateforme>**. ▪ Si vos informations d'identification se trouvent dans plusieurs coffres-forts, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :<ID d'informations d'identification>**.
URL du jeton OAuth	URL qui spécifie le point de terminaison permettant d'obtenir le jeton d'accès du serveur OAuth.

n. Sélectionnez **Configurer la connexion**.

2. Configurez une connexion manuellement.

a. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.

b. Sélectionnez **Nouveau**.

c. Sélectionnez **Se connecter à un fournisseur OAuth tiers à l'aide d'un coffre externe**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Remplissez le formulaire.

Détails du nouveau registre d'application

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement du registre d'application. Par exemple, entrez : demande de jeton OAuth 2.0 via l'application MID.
Application	Option permettant de spécifier les noms des applications qui peuvent accéder à ce registre d'application. Le champ est en lecture seule.
Type d'accord par défaut	Méthode par défaut pour obtenir le jeton d'accès par l'application cliente à partir du serveur OAuth. Le type d'accord par défaut et en lecture seule est Informations d'identification du client.
Accessible depuis	Option permettant de spécifier quelles applications peuvent accéder à ce registre d'application.
URL de jeton	URL qui spécifie le point de terminaison permettant d'obtenir le jeton d'accès du serveur OAuth.
Envoyer les informations d'identification	Option permettant de spécifier la méthode d'envoi de l'OAuth 2.0 dans le corps de la demande.
Commentaires	Saisissez les commentaires associés.

e. Dans la colonne **Périmètre OAuth** , créez un ou plusieurs champs d'application OAuth en procédant comme suit.

i. Dans la colonne Nom, double-cliquez sur le champ et entrez un nom du périmètre OAuth.

ii. Dans la colonne Périmètre OAuth, double-cliquez sur le champ et entrez le périmètre.

f. Sélectionnez **Soumettre**.
Vous avez créé un profil d'entité OAuth et le registre d'application.

g. Accédez à la **Tous** > **Centre d'intégration** > **Connexions et informations d'identification** > **Informations d'identification**.

h. Sélectionnez **Nouveau**.

i. Sélectionnez **Informations d'identification OAuth 2.0**.

j. Sélectionnez la vue de stockage externe.

> **Important :**
> Sélectionnez **la vue du stockage externe** uniquement si la vue est différente de celle d'un formulaire de stockage externe des informations d'identification OAuth 2.0.

k. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification OAuth 2.0

Champ	Description
Nom	Nom de l'enregistrement d'informations d'identification.
Concerne	Option permettant de spécifier si l'enregistrement des informations d'identification est applicable à tous les serveurs MID ou à un serveur MID spécifique. Si précis, ajoutez les MID Server. Choisissez l'une des options suivantes. ▪ Tous les serveurs MID : le serveur MID est automatiquement sélectionné dans une collection de serveurs MID. ▪ Serveurs MID spécifiques : option permettant de spécifier un ou plusieurs serveurs MID.
Serveurs MID	Option permettant de spécifier un ou plusieurs serveurs MID. **Remarque :** Ce champ s'affiche si vous sélectionnez **Serveurs MID spécifiques** dans le champ S'applique à.
Actif	Option permettant de spécifier si l'enregistrement des informations d'identification est disponible pour utilisation. Il est disponible par défaut.
Profil de l'entité OAuth	Option permettant de spécifier un profil d'entité OAuth que les informations d'identification utilisent. Sélectionnez le profil d'entité OAuth que vous avez créé ci-dessus. Consultez Configurer un profil d'entité OAuth.
Banque d'identifiants externes	Option permettant de spécifier que les informations d'identification sont stockées dans un stockage externe et non dans l'instance ServiceNow. **Important :** Confirmez que l'option est sélectionnée.
ID de certification	Option permettant de spécifier l'identificateur d'informations d'identification pour le compte CyberArk qui détient l'ID client et le secret client. Pour afficher la procédure d'obtention de l'identificateur d'identification, reportez-vous à la section Configurer les informations d'identification OAuth 2.0 sur CyberArk.
Chambre forte de stockage des informations d'identification	Option permettant de spécifier le nom du coffre de stockage des informations d'identification externe. Vérifiez que vous avez sélectionné CyberArk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement des informations d'identification.

m. Créez un alias de connexion et d'informations d'identification.
Pour connaître les étapes, reportez-vous à la section Créer un alias de connexion et d'informations d'identification.

n. Accédez à la **Tous** > **Centre d'intégration** > **Connexions**.

o. Sélectionnez **Nouveau**.

p. Sélectionnez **Connexion HTTP(s)**.

q. Remplissez le formulaire.

Formulaire de connexion

Champ	Description
Nom	Nom unique de cette connexion HTTP(s).
Actif	Option permettant de définir la connexion que vous créez active. L'option est sélectionnée par défaut.
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion. Sélectionnez les informations d'identification que vous avez créées ci-dessus.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Générateur d'URL	Entrez manuellement l'URL de connexion ou utilisez le système pour créer l'URL en fonction des entrées. Il n'est pas coché par défaut. Si cette option est cochée, l'URL de connexion est calculée à partir des champs suivants : ▪ Authentification réciproque : cochez la case si l'authentification réciproque est utilisée. ▪ Protocole : si l'authentification réciproque n'est pas utilisée, entrez protocole. La valeur par défaut est HTTPs. ▪ Profil du protocole : si l'authentification réciproque est utilisée, entrez le profil du protocole à partir de sys_protocol_profile. ▪ Hôte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Port ▪ Chemin de base : chemin d'accès de la chaîne de connexion. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est générée : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : Profil du protocole + :// + hôte :port +URL
URL de connexion	Si l'option Générateur d'URL est décochée, entrez l'URL de connexion dans ce champ. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est générée : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : Profil du protocole + :// + hôte :port +URL
Utiliser un serveur MID	Option permettant de spécifier que vous souhaitez envoyer des demandes de jetons OAuth via un serveur MID. **Important :** Confirmez que l'option est sélectionnée.
Délai de connexion	Nombre de millisecondes pendant lesquelles le système attend une connexion de l'hôte réussie. Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Laissez ce champ vide pour utiliser la valeur de délai de connexion par défaut du système.
Sélection de MID	Option permettant de spécifier l'une des options suivantes. ▪ Sélectionner automatiquement Serveur MID : effectue une sélection à partir des serveurs MID en fonction des critères de Serveur MID, qu'ils soient membres d'une grappe ou non. ▪ Serveur MID spécifique : sélectionnez manuellement un serveur MID. ▪ Grappe MID spécifique : la réaffectation automatique à un autre serveur MID sélectionne uniquement parmi les membres de la grappe spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Important : Vérifiez que le serveur MID que vous sélectionnez réside sur la même machine que le client CyberArk AIM configuré pour accéder au coffre-fort CyberArk. Consultez Configurer le coffre-fort CyberArk et installer l'API AIM.
Options	Option permettant de sélectionner une ou plusieurs options de Serveur MID. Les options définissent les fonctions spécifiques d'un serveur MID dans une plage d'adresses IP, ce qui permet à une application de sélectionner le serveur MID le plus approprié. Sélectionnez l'icône des options (+) pour sélectionner une ou plusieurs options. **Remarque :** ▪ Vérifiez que le serveur MID que vous sélectionnez réside sur la même machine que le client CyberArk AIM configuré pour accéder au coffre-fort CyberArk. Consultez Configurer le coffre-fort CyberArk et installer l'API AIM. ▪ Cette option s'affiche si vous sélectionnez **Sélectionner automatiquement Serveur MID** dans le champ Sélection MID.
Serveur MID	Sélectionnez manuellement un serveur MID. Cette option s'affiche si vous sélectionnez Serveur MID spécifique dans le champ Sélection MID.
Grappe MID	Sélectionner manuellement une grappe MID. Cette option s'affiche si vous sélectionnez Grappe MID spécifique dans le champ Sélection MID.
Application MID	Option permettant de spécifier une application MID ou d'accepter le choix d'application par défaut. **Remarque :** Cette option s'affiche si vous sélectionnez **Sélectionner automatiquement Serveur MID** dans le champ Sélection MID. Par défaut, l'option **TOUT** est sélectionnée.

r. Sélectionnez **Soumettre**.
Vous avez créé un enregistrement de connexion HTTP(s).

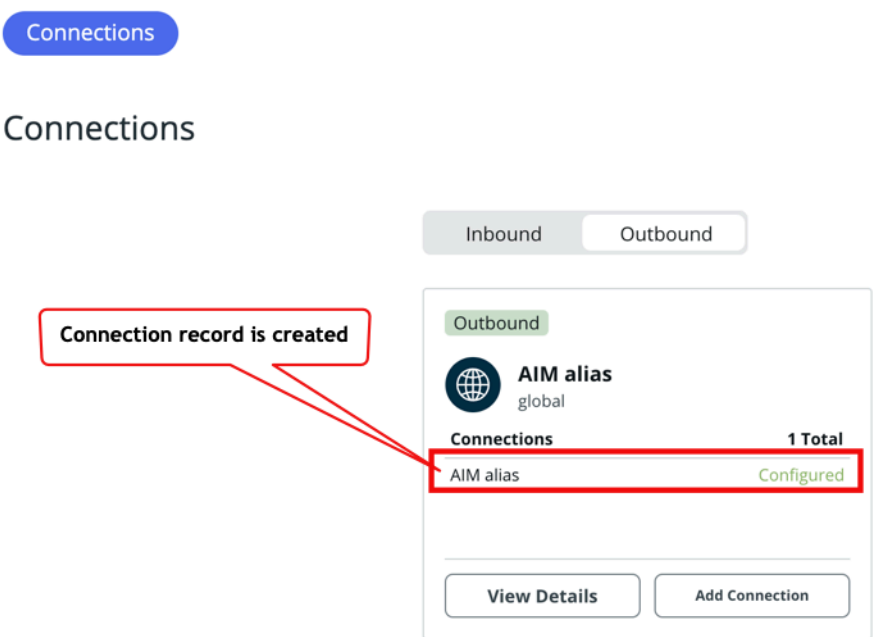
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

s. Accédez à la **Tous** > **Automatisation des processus** > **Centre d'intégration** > **Tableau de bord des connexions**.

t. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement de connexion que vous avez créé.
L'enregistrement de l'alias de connexion s'affiche.

L'enregistrement de connexion OAuth 2.0 est créé



Algorithmes d'authentification

Vérifier l'identité de l'expéditeur à l'aide des algorithmes d'authentification

Autorisez les étapes d'intégration pour s'authentifier auprès des services Web qui nécessitent des mécanismes de connexion ou d'informations d'identification complexes ou non standard. Associez des algorithmes d'authentification aux alias d'informations d'identification et de connexion pour réduire ou éliminer la nécessité de configurer manuellement les étapes d'intégration.

Vous pouvez utiliser un algorithme d'authentification pour générer des données d'authentification personnalisées pour vos étapes d'intégration. Les étapes d'intégration peuvent utiliser ces données dynamiques pour créer tous les artefacts personnalisés nécessaires pour s'authentifier auprès du service Web cible. Par exemple, une étape REST peut créer un en-tête d'authentification, des paramètres de requête ou un jeton.

Les algorithmes d'authentification prennent en charge les étapes suivantes :

- Étape Obtenir des informations sur la connexion
- Étape REST
- Étape SOAP

Pour plus d'informations, consultez la section Étapes d'intégration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types d'algorithmes d'authentification

- **Amazon Signature Version 4** : il s'agit d'un algorithme d'authentification prédéfini permettant de se connecter à Amazon Web Services.
- **Authentification personnalisée** : il s'agit d'un modèle que les développeurs peuvent utiliser pour créer leurs propres algorithmes d'authentification.

Pour en savoir plus sur la configuration de l'algorithme d'authentification, reportez-vous à la section Configurer un algorithme d'authentification.

Scripts

Les scripts d'authentification d'instance se trouvent sur les scripts d'instance qui font partie de la *sys_script_include* table.

Scripts d'authentification d'instance

RequestAuthInternal	Script en lecture seule sur l'instance, qui prend en charge la génération de la signature AWS V4 ou de l'authentification personnalisée envoyée avec la demande sortante.
RequestAuthAWSV4Signer	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer la signature AWS V4.
RequestAuthTwitterSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature Twitter à l'aide d'OAuth 1.0a.
RequestAuthSampleCustomSigner	Exemple de script étendant RequestAuthInternal pour comprendre comment écrire un signataire personnalisé sur une instance.

Les scripts d'authentification MID se trouvent sur la partie des scripts MID de *ecc_agent_script_include* la table.

Scripts d'authentification MID

RequestAuthInternal	Script en lecture seule sur MID, qui prend en charge la génération de la signature AWS V4 ou de l'authentification personnalisée envoyée avec la demande sortante.
RequestAuthAWSV4MIDSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer la signature AWS V4.
RequestAuthTwitterSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature Twitter à l'aide d'OAuth 1.0a.
RequestAuthSampleMidCustomSigner	Exemple de script étendant RequestAuthInternal pour comprendre comment écrire un signataire personnalisé sur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

API JavaScript

L'API JavaScript pour l'algorithme d'authentification est la suivante.

- AuthCredential
- HttpRequestAuthedData
- HttpRequestData
- RequestAuthAPI

Configurer un algorithme d'authentification

Configurez un algorithme d'authentification afin de pouvoir signer les demandes HTTP sortantes.

Avant de commencer

Un include de script doit être configuré avant de configurer un algorithme d'authentification.
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Remplissez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs disponibles.

Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante.
Description	Description de ce que fait votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script.
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Découverte].

3. Cliquez sur **Envoyer**.

Configurer un algorithme personnalisé basé sur la Amazon signature

Générez les données basées sur la Amazon signature nécessaires pour vous authentifier auprès d'un service Web en exécutant un script.

Avant de commencer

- Base de connaissances JavaScript
- Connaissances REST
- Connaissances sur l'API du service Web cible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connaissances en matière de connexion, d'informations d'identification et d'alias
- Rôle requis : Développeur

Pourquoi et quand exécuter cette tâche

Utilisez un alias de connexion et d'informations d'identification et Amazon un algorithme basé sur Signature Version 4 pour l'authentification.

Procédure

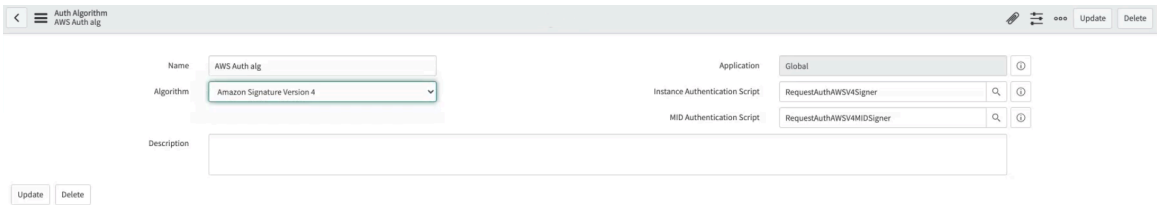
1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Remplissez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs disponibles.

Formulaire d'authentification

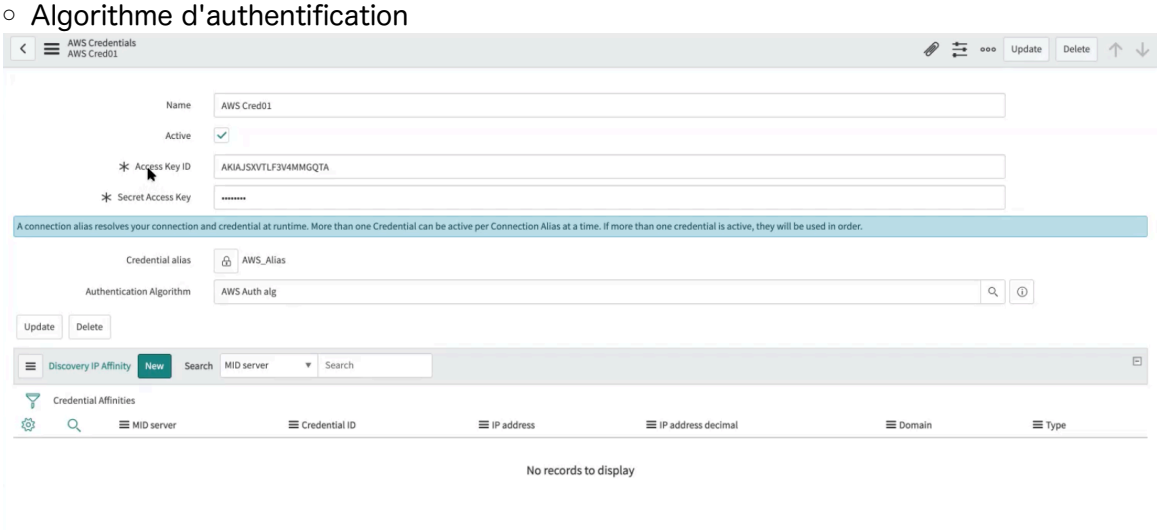
Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **Amazon Signature Version 4**.
Description	Description de ce que fait votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script. Dans le cas de l'algorithme **Amazon Signature Version 4** , choisissez **RequestAuthAWSV4Signer**. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Remarque :** Pour en savoir plus sur le script, cliquez sur l'icône d'informations en regard du champ. Les détails du script, tels que le nom, le nom de l'API, l'application, l'accessible depuis, le script, etc. s'affichent.
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Découverte]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tous** > **Connexions et informations d'identification** > **Informations d'identification**.
5. Cliquez sur **Nouveau**.
6. Créez des AWS informations d'identification avec l'algorithme d'authentification.
   Dans ce cas, **AWS Auth alg**.
7. Spécifiez les éléments suivants :
   - Nom
   - Actif
   - ID de clé d'accès
   - Clé d'accès secrète
   - Alias d'identification
   - Algorithme d'authentification



8. Cliquez sur **Mettre à jour**.

Résultats

En fonction des scripts et de l'algorithme d'authentification sélectionnés, les informations d'identification configurées (**ID de clé d'accès et cléd'accès secrète**) ou les informations d'identification de l'utilisateur (**ID de clé d'accès**, **clé d'accès secrète** et **jeton de session**) génèrent une Amazon signature V4 qui est envoyée en tant que demande sortante par ServiceNow le fournisseur (dans ce cas).AWS

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

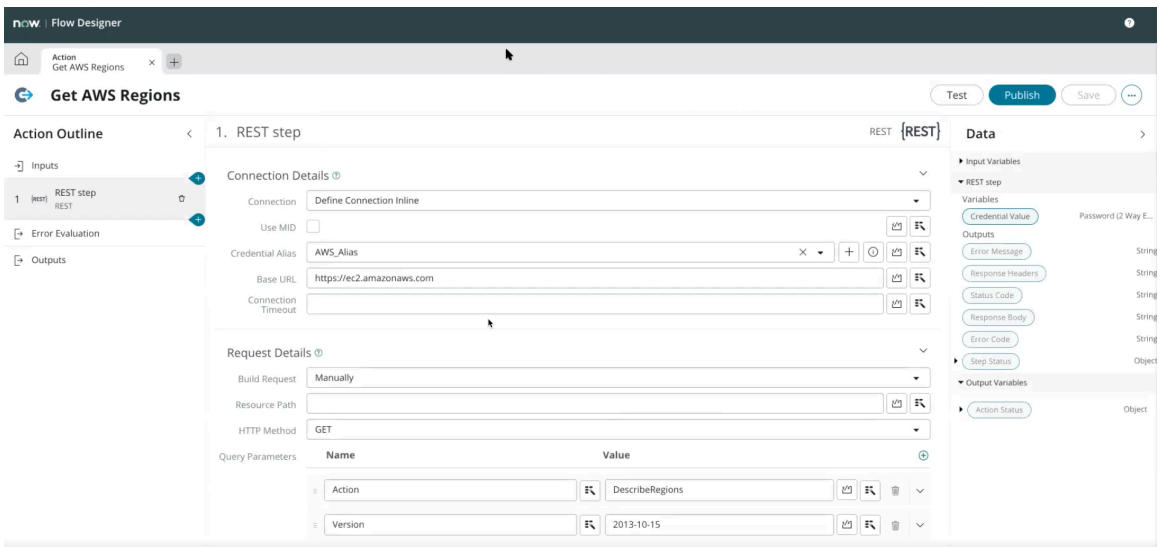
Example: Étape REST avec AWS

Remarque :
Amazon L'authentification basée sur la signature V4 peut également être utilisée à partir de l'arrière-plan du script.

Action : obtenir les AWS régions

Saisissez l'étape REST comme AWS suit :

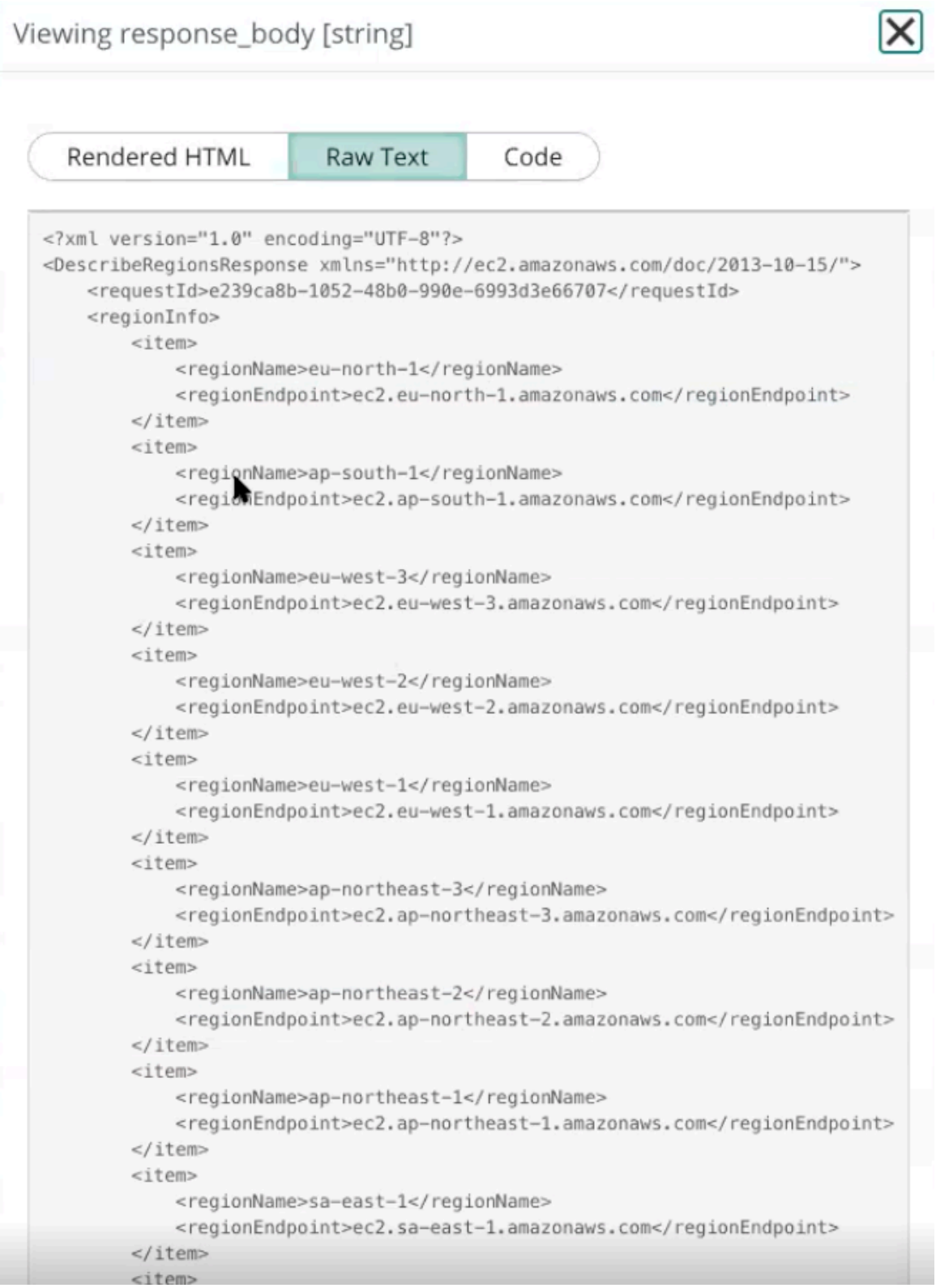
- **Alias d'informations d'identification** : l'alias créé pour AWS.
- **URL de base** : détails de l'URL de base à partir de AWS.
- **Méthode HTTPS** : Dans ce cas, il s'agit de la méthode GET.
- **Paramètres de requête** : **action** en tant que **DescribeRegions**.



Vous pouvez tester l'action, les régions associées s'affichent. Le corps de la réponse est le suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Amazon V4 est défini avec un ensemble standard d'algorithmes qui prennent en charge le mécanisme d'authentification. Cet algorithme, lorsqu'il est utilisé, ajoute la signature en tant qu'en-tête d'autorisation pour l'authentification (requête HTTP) à l'aide de l'étape REST.

Configurer un algorithme d'authentification personnalisé

Générez les données personnalisées nécessaires pour vous authentifier auprès d'un service Web en exécutant un script.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Base de connaissances JavaScript
- Connaissances REST
- Connaissances sur l'API du service Web cible
- Connaissances en matière de connexion, d'informations d'identification et d'alias
- Rôle requis : Développeur

Pourquoi et quand exécuter cette tâche

Utilisez un alias de connexion et d'informations d'identification et un algorithme basé sur une authentification personnalisée pour l'authentification.

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Remplissez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs disponibles.

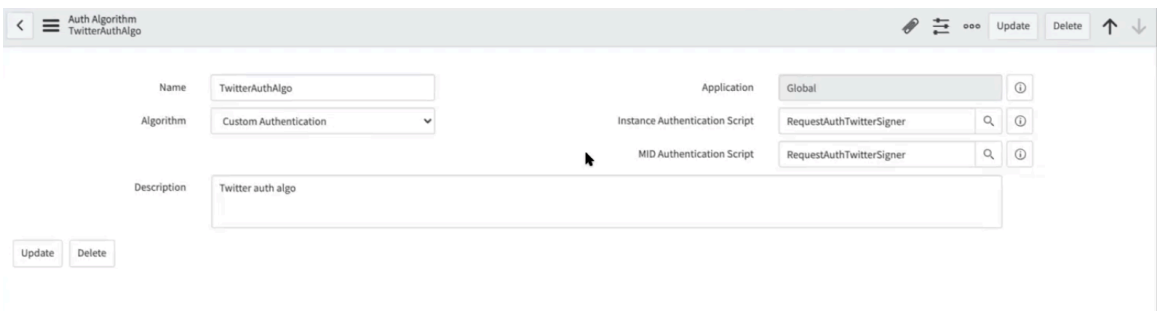
Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **l'authentification personnalisée**.
Description	Description de ce que fait votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Remarque :** ○ Pour en savoir plus sur le script, cliquez sur l'icône d'informations en regard du champ. Les détails du script, tels que le nom, le nom de l'API, l'application, l'accessible depuis, le script, etc. s'affichent. ○ En cas d'authentification personnalisée avec Twitter, vous pouvez choisir **RequestAuthTwitterSigner**, car il utilise une méthode d'authentification OAuth 1.0a. Cela nécessite des informations telles que **la clé API et le secret,** ainsi que le **jeton d'accès et le secret** qui peuvent être utilisés pour créer des signatures à transmettre dans un en-tête d'autorisation. Pour plus d'informations, consultez Authentification dans Twitter .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Découverte]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

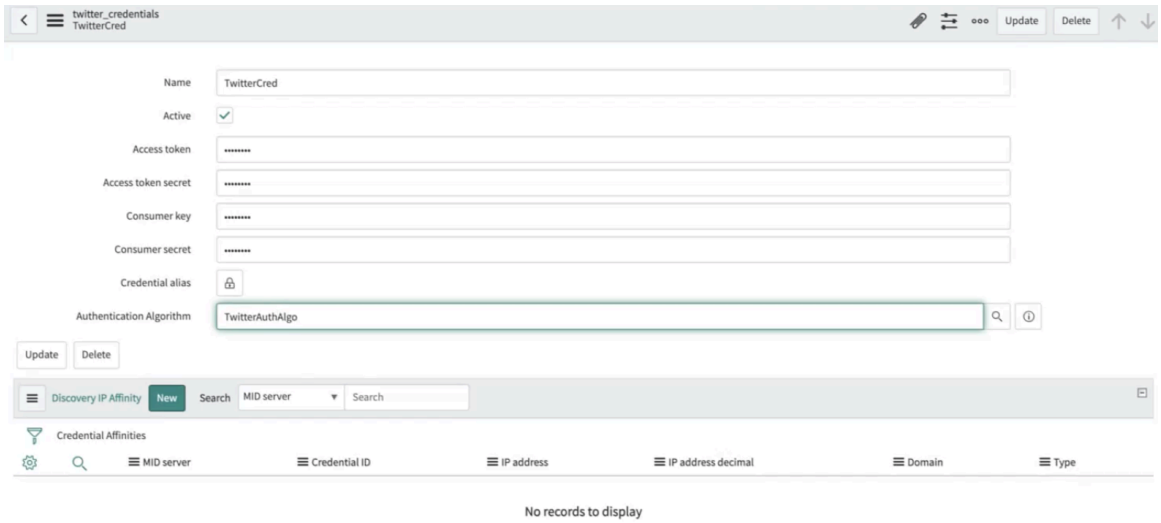


En fonction des scripts sélectionnés et de l'algorithme d'authentification, les informations d'identification configurées sont envoyées en tant que demande sortante au ServiceNow fournisseur.

3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tous** > **Connexions et informations d'identification** > **Informations d'identification**.
5. Cliquez sur **Nouveau**.
6. Créez des Twitter informations d'identification avec l'algorithme d'authentification.
   Dans ce cas **, TwitterAuthAlgo**.
7. Spécifiez les champs :
   - Nom
   - Actif
   - Jeton d'accès
   - Secret du jeton d'accès
   - Clé du consommateur
   - Secret du consommateur
   - Alias d'identification
   - Algorithme d'authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Cliquez sur **Mettre à jour**.

Example: Étape REST avec Twitter

Dans le cas de Twitter, vous devez vous assurer que les spokes ou les informations d'identification suivants sont disponibles :

- Jeton d'accès
- Secret du jeton d'accès
- Clé du consommateur
- Secret du consommateur
- Algorithme d'authentification

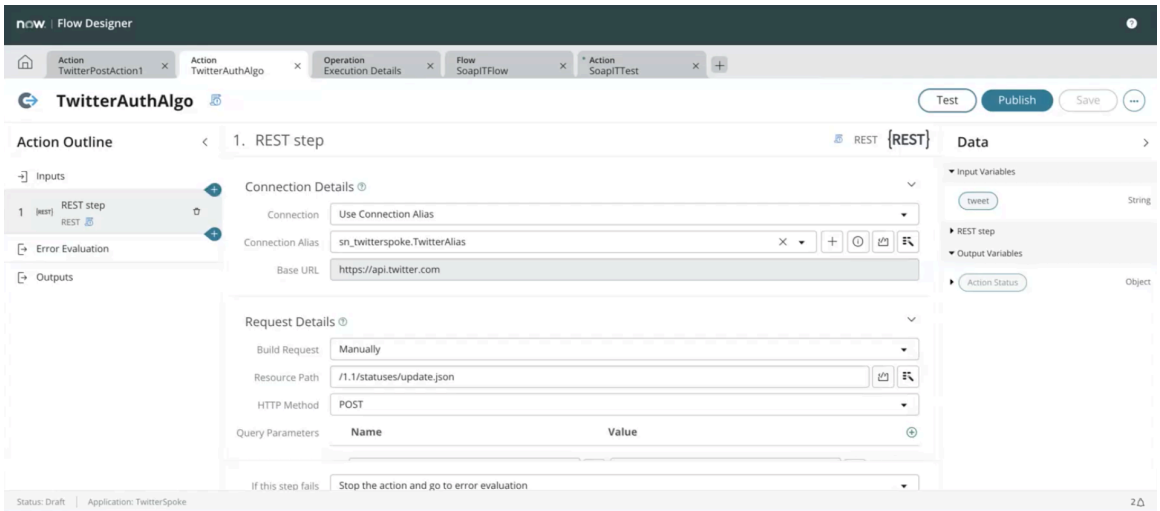
Action : TwitterAuthAlgo.

Saisissez l'étape REST comme Twitter suit :

- **Alias d'informations d'identification** : l'alias créé pour Twitter.
- **URL de base** : détails de l'URL de base à partir de Twitter.
- **Méthode HTTPS** : Dans ce cas, il s'agit de la méthode POST. Poster un tweet.
- **Paramètres de requête** : **Action** en tant que **tweet**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez tester l'action. Le tweet est publié sur la Twitter page.

Vérifier la relation des services IP pour Discovery et Orchestration

Vous pouvez rechercher dans la table Services IP une liste d'adresses IP associées à un protocole.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La table Services IP mappe un port sur un protocole. Plusieurs mappages sont fournis par défaut pour les combinaisons port-protocole couramment utilisées, tels que le port 80 pour HTTP, le port 22 pour SSH et le port 161 pour SNMP.

Une propriété système appelée `glide.discovery.ip_service_affinity` permet à Découverte de mémoriser le dernier port de l'adresse IP ayant été détecté.

Important :
Vous ne devez pas modifier les services IP à moins que votre organisation n'utilise des ports personnalisés.

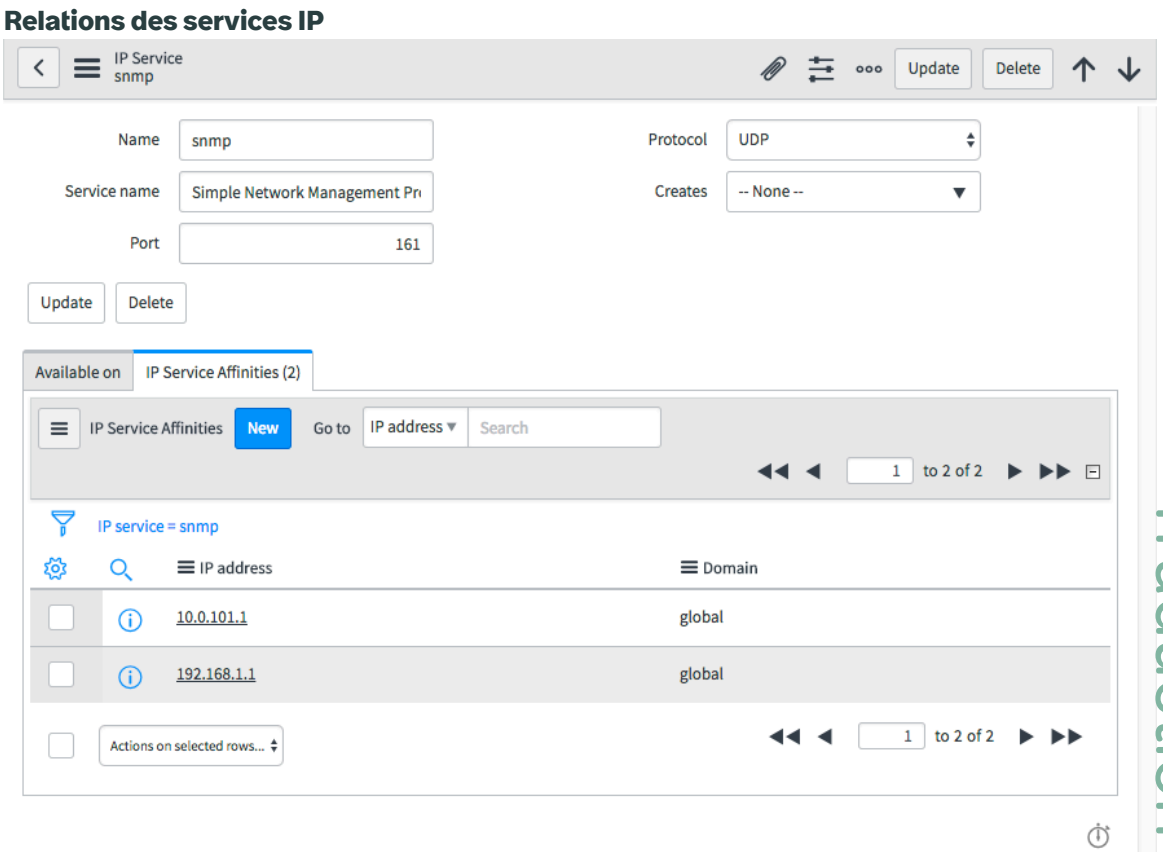
Procédure

1. Accédez à la **Tous** > **Définition de découverte** > **Services IP**.
2. Filtrez la liste pour rechercher le service IP approprié.
3. Cliquez sur le nom du service pour accéder à la page de ce service IP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur l'onglet **Relations des services IP** pour obtenir la liste d'adresses IP associées à ce service.



Contrôle d'accès ServiceNow®

Le module d'extension Contrôle d'accès SNC (com.snc.snc_access_control) vous permet de contrôler quels Service client et assistance employés peuvent accéder à votre instance et quand.

Découvrir le contrôle d'accès ServiceNow



Activer le contrôle d'accès ServiceNow



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur les fonctionnalités du contrôle d'accès ServiceNow® .

Contrôle d'accès actif ServiceNow® .

Configurer le contrôle d'accès ServiceNow



Comprendre comment configurer ServiceNow® le contrôle d'accès.

Journalisation d'audit



Apprenez et examinez la journalisation de l'audit de contrôle d'accès ServiceNow® .

Traduction automatique

Contrôle d'accès Exploree ServiceNow®

Le module d'extension Contrôle d'accès SNC (com.snc.snc_access_control) vous permet de contrôler quels Service client et assistance employés peuvent accéder à votre instance et quand.

Lorsque vous activez le module d'extension pour la première fois, Service client et assistance les employés ne peuvent pas se connecter à l'instance. Tous les employés actuellement connectés Service client et assistance restent connectés. Vous créez des enregistrements dans la table Contrôle d'accès SNC qui accordent l'accès à des employés SNC spécifiques ou à tous les employés.

Le module d'extension empêche Service client et assistance le personnel d'accéder aux instances sans votre autorisation expresse. Toutefois, d'autres membres du personnel d'exploitation autorisés ServiceNow , dans leur capacité à prendre en charge et à gérer le produit et à vérifier son utilisation, sont tenus d'effectuer des actions administratives sur l'infrastructure sous-jacente. Cette infrastructure comprend des serveurs et des bases de données, entre autres composants de l'infrastructure qui composent la solution SaaS. Cette méthode d'accès est entièrement auditable et suivie.

Ce module d'extension vous permet de restreindre l'accès à votre instance sans votre autorisation expresse, de sorte que cela peut affecter les niveaux de service d'assistance et

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le SLA de disponibilité. La disponibilité du SLA est ensuite mesurée à partir du moment où le personnel de support est autorisé à accéder à votre instance.

Sécurité de la connexion

La sécurité des connexions des employés autorisés Service client et assistance aux instances utilise des jetons chiffrés générés par un serveur sécurisé. Seuls les employés correctement authentifiés Service client et assistance ont accès à une instance. Sans le module d'extension SNC Access Control, le serveur de sécurité garantit que les droits d'accès sont appliqués sur hi.service-now.com. Lorsque le module d'extension est activé, les jetons de connexion chiffrés doivent correspondre aux noms de la liste d'accès fournie par le module d'extension, à l'aide des critères définis dans ces enregistrements. Cette méthode d'authentification vous permet de déterminer précisément quels Service client et assistance employés peuvent accéder à leurs instances et quand ils peuvent le faire.

L'architecture choisie pour ce système comporte plusieurs fonctionnalités conçues pour améliorer la sécurité de vos instances :

Serveur de sécurité

Le serveur de sécurité est un hôte Linux verrouillé auquel seul le ServiceNow personnel de sécurité peut accéder. Ce serveur est le seul système qui a accès à la clé de chiffrement privée critique nécessaire pour produire les jetons de connexion. En utilisant cette compartimentation (une pratique de sécurité standard), la clé privée est protégée, même dans le cas peu probable où un attaquant compromettrait l'instance HI.

Utilisateur synthétique

L'installation sur les instances qui permet aux employés autorisés Service client et assistance de se connecter à leur instance ne nécessite pas la mise en service d'un compte sur cette instance. Il n'y a pas d'enregistrement utilisateur mis en service, ni d'informations d'identification permanentes ou persistantes. Au lieu de cela, un utilisateur synthétique est créé pour chaque Service client et assistance connexion d'employé. Cet utilisateur n'existe qu'en mémoire et ne fournit aucun privilège permanent. Si le module d'extension Contrôle d'accès SNC est activé, vous pouvez retirer l'autorisation de n'importe quel Service client et assistance employé à tout moment.

Jetons

Les jetons de sécurité sont spécifiques à une instance et à un employé particulier Service client et assistance . En outre, le mécanisme qui génère les jetons ne fonctionne qu'avec les connexions réelles Service client et assistance des employés à HI, et non avec les utilisateurs dont l'identité a été empruntée. Une fois qu'un jeton de sécurité est généré, seul un employé spécifique Service client et assistance peut l'utiliser pour se connecter à une instance.

Limite de temps

Les jetons de sécurité expirent quatre heures après leur génération. Cette expiration limite l'utilité des jetons détournés, qui ne peuvent être utilisés que pendant cette courte période.

Connexion

Les connexions des Service client et assistance employés aux instances sont enregistrées comme un événement de connexion.

- Chaque action effectuée par l'employé connecté Service client et assistance est ajoutée au journal des transactions dans la base de données.
- Il est également ajouté au journal d'instance sur le système de fichiers, qui est inaccessible à la plupart ServiceNow des employés.
- Service client et assistance Les connexions et les actions des employés sont facilement identifiables, car les noms d'utilisateur se terminent tous par @snc (comme frodo.baggins@snc).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

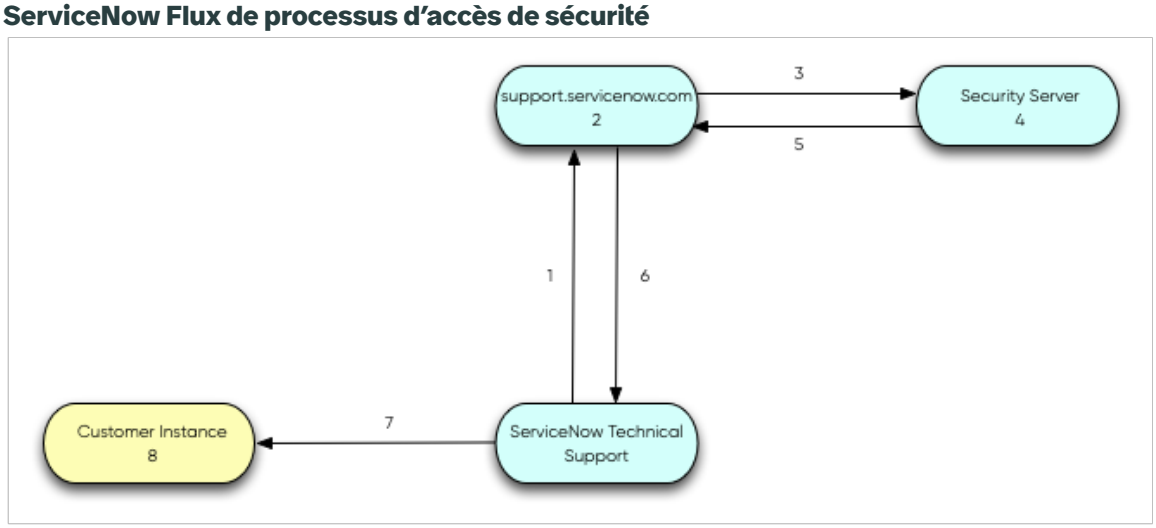
Ces actions vous fournissent une journalisation de sécurité facile à utiliser, robuste et fiable pour l'accès des non-employés.

Flux de traitement de la sécurité

Lorsqu'un Service client et assistance employé souhaite se connecter à une instance, le flux de traitement de la sécurité est le suivant :

1. Un Service client et assistance technicien demande une connexion pour l'instance via hi.service-now.com.
2. HI vérifie que le technicien dispose du rôle approprié pour autoriser l'accès aux instances.
3. Si l'utilisateur dispose du rôle approprié, HI envoie la demande d'accès au serveur de sécurité.
4. Le serveur de sécurité vérifie que la demande provient de l'adresse IP HI et évalue la demande (utilisateur, rôle et adresse IP du demandeur). Si la demande est valide, le serveur de sécurité l'approuve et crée un jeton. Ce jeton contient le nom d'utilisateur, les rôles, l'ID d'instance et l'heure (le début de la durée de vie du jeton de 4 heures). Enfin, le serveur de sécurité crypte le jeton avec la clé de chiffrement privée.
5. Le serveur de sécurité envoie le jeton chiffré à HI.
6. Hi envoie le jeton au navigateur du technicien de support.
7. Le navigateur du technicien de support initie une connexion dans l'instance, à l'aide du nom d'utilisateur spécial se terminant par @snc.
8. L'instance utilise la clé publique pour déchiffrer le jeton. Pour vérifier le jeton, l'instance le fait correspondre au nom d'utilisateur fourni à l'étape précédente, à l'ID de l'instance et à la fenêtre de temps autorisée. Si le module d'extension Contrôle d'accès SNC est activé, l'instance vérifie que l'utilisateur est :
   - Énuméré(e/s)
   - Actif
   - Configuré pour accéder à l'instance dans la fenêtre de temps actuelle
9. Si l'utilisateur est authentifié, l'instance crée un *utilisateur synthétique* en mémoire avec les rôles donnés. Cet utilisateur ne persiste pas après l'expiration du délai, la déconnexion de l'utilisateur ou le redémarrage de l'instance.

ServiceNow Flux de processus d'accès de sécurité



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journalisation d'audit

La journalisation suivante suit les connexions et l'activité des Service client et assistance employés :

- Journaux des événements : les journaux des événements affichent toutes les Service client et assistance connexions à une instance.
- Journaux des transactions : les journaux des transactions affichent toutes les activités sur l'instance, y compris les efforts de suppression des journaux.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Activer le module d'extension du contrôle d'accès SNC [Mis à jour dans Centre de sécurité 1.3] Paramètres de la sécurisation renforcée de la sécurité de l'instance.

Activer ServiceNow® le contrôle d'accès

Vous demandez l'activation du module d'extension SNC Access Control (com.snc.snc_access_control).

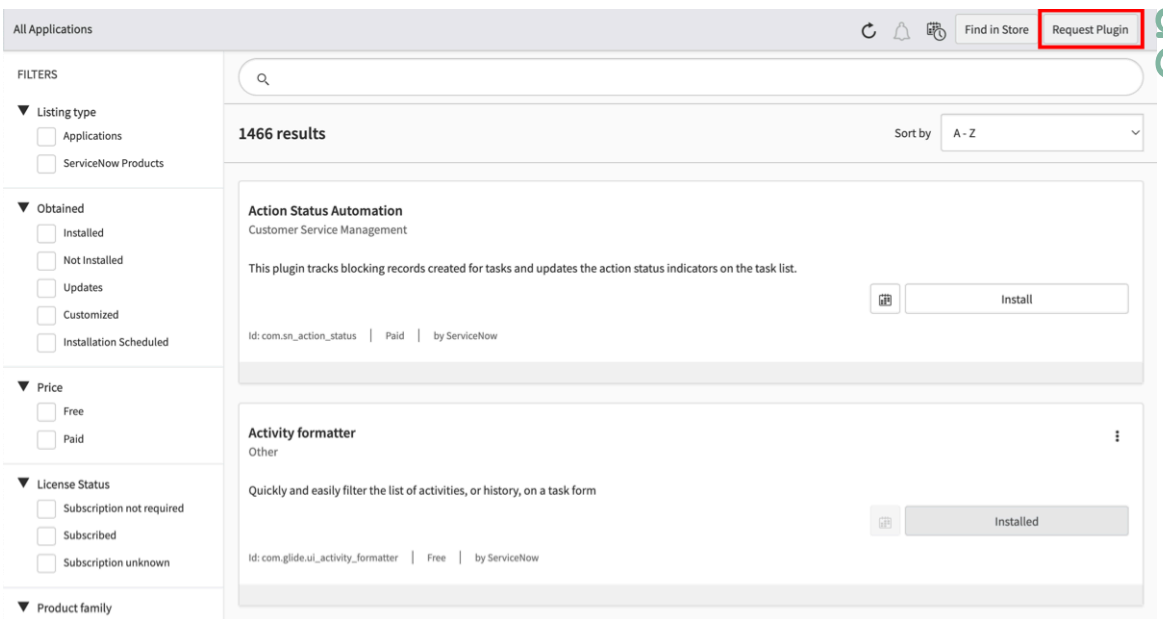
Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Il existe deux façons de demander un module d'extension :

- Accéder directement au Now Support catalogue de services en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

Procédure

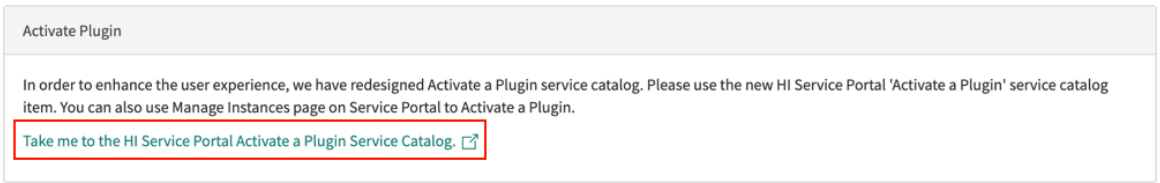
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

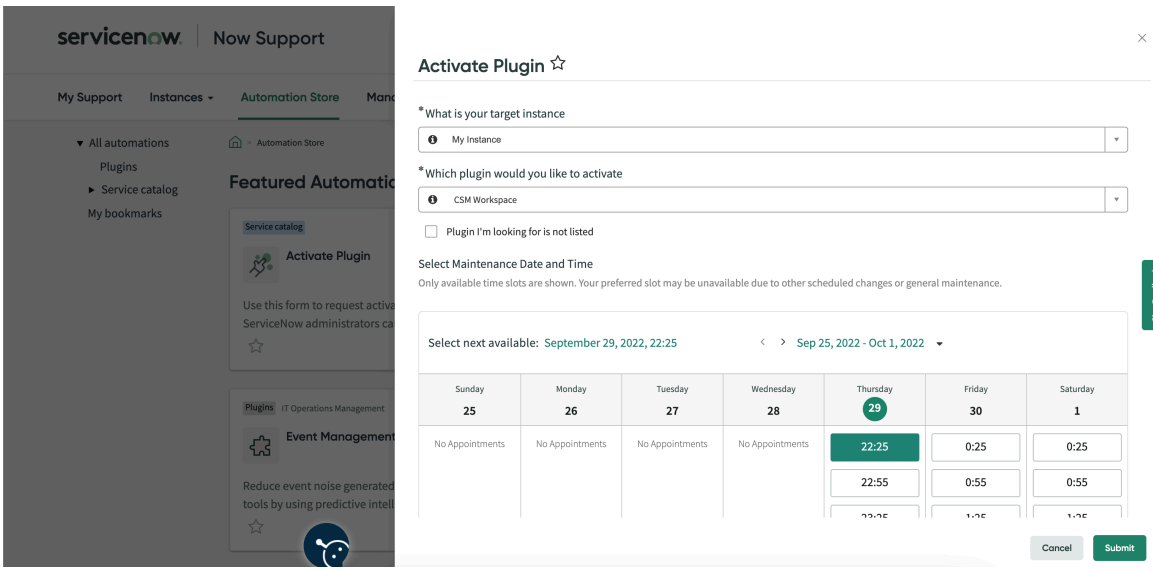
Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Activer le module d'extension



7. Sélectionnez **Soumettre**.
   Pour plus de détails sur la demande d'un module d'extension, consultez Demander un module d'extension à partir de l'article Catalogue de services [KB0751715] dans le Now Support Base de connaissances.

Configurer ServiceNow® le contrôle d'accès

Configurez un enregistrement de contrôle d'accès pour spécifier un ou Service client et assistance plusieurs employés qui ont l'autorisation de se connecter dans votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :

Le module d'extension Contrôle d'accès SNC (com.snc.snc_access_control) empêche Service client et assistance le personnel d'accéder aux instances sans votre autorisation expresse. Toutefois, d'autres membres du personnel d'exploitation autorisés ServiceNow , dans leur capacité à prendre en charge et à gérer le produit, sont tenus d'effectuer des actions administratives sur l'infrastructure sous-jacente. Cette infrastructure comprend des serveurs et des bases de données, entre autres composants de l'infrastructure qui composent la solution SaaS. Cette méthode d'accès est entièrement auditable et suivie.

Ce module d'extension vous permet de restreindre l'accès à votre instance sans votre autorisation expresse, de sorte que cela peut affecter les niveaux de service d'assistance et le SLA de disponibilité. La disponibilité du SLA est ensuite mesurée à partir du moment où le personnel de support est autorisé à accéder à votre instance.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Contrôle d'accès SNC**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs de formulaire (consultez la table).
4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôle d'accès SNC

Champs de formulaire	Description
Nom	Nomme chaque Service client et assistance employé qui a l'autorisation de se connecter dans cette instance. ○ Exprimez les noms sous la forme prenom.nom en minuscules, séparés par un point (par exemple, john.smith). Chaque nom doit avoir un enregistrement utilisateur correspondant dans *support.servicenow.com*. ○ Si plusieurs Service client et assistance employés ont l'autorisation de se connecter dans cette instance, saisissez plusieurs noms et séparez-les par des virgules. ○ Pour activer les droits de connexion de tous les Service client et assistance employés pour accéder à l'instance, entrez un astérisque (*) à la place du nom. ○ Si vous avez l'intention de restreindre Service client et assistance l'accès des employés à l'instance, les valeurs du champ **Nom** ne doivent pas comporter d'astérisque (*) dans le champ.
Motif	Champ explicite qui décrit pourquoi vous accordez une autorisation d'accès. Ce champ est facultatif.
Début	Spécifie la date et l'heure de début de la période pendant laquelle les employés spécifiés Service client et assistance ont un accès à la connexion. Ce champ est obligatoire.
Fin	Spécifie la date et l'heure de fin de la période pendant laquelle les employés spécifiés Service client et assistance ont un accès à la connexion. Ce champ est obligatoire.
Actif	Contrôle si cet enregistrement d'autorisation est actif. La valeur par défaut est Actif.

Journalisation d'audit

La journalisation suivante suit les connexions et l'activité des ServiceNow employés.

Journaux des événements	Les journaux des événements affichent toutes les ServiceNow connexions à une instance client.
Journaux de transactions	Les journaux des transactions affichent toute l'activité sur l'instance, y compris les efforts de suppression des journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identité

En savoir plus sur les identités dans l’instance.

Analyseur d'accès



L’analyseur d’accès est un outil de diagnostic de ServiceNow® qui vous aide à déterminer les raisons pour lesquelles un utilisateur a accès à une ressource.

Identité globale



Application de l’App Store qui vous permet de mettre à jour les attributs d’utilisateur d’une instance à une instance (plusieurs instances).

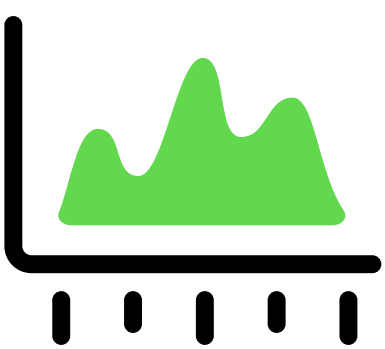
Global Identity est une application de ServiceNow® de stockage qui permet de mettre

Identity Center



Identity Center vous permet de surveiller, gérer et minimiser les risques basés sur l’identité et les failles de sécurité.

Système de gestion des identités interdomaines (SCIM)



L’API SCIM (System for Cross-domain Identity Management) fournit des points de terminaison pour créer, lire, mettre à jour et supprimer des opérations sur des utilisateurs et des groupes à l’aide du protocole SCIM.

Audit d'identité et d'accès



Utilisez l’audit d’identité et d’accès pour comprendre les changements apportés à un utilisateur, un groupe, un rôle et un ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyseur d'accès

ServiceNow® Access Analyzer est un outil de diagnostic d’accès qui permet d’afficher les autorisations d’une identité pour une ressource.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Access Analyzer.

Utiliser



Comprendre comment utiliser l’analyseur d’accès.

Évaluation des autorisations



Sachez comment les autorisations sont évaluées.

Forum Aux Questions



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenez des détails sur les questions fréquemment posées sur l'analyseur d'accès.

Exploration de l'analyseur d'accès

Analysez les identités sur l'instance ServiceNow .

ServiceNow Access Analyzer est une application qui aide les administrateurs à afficher les autorisations pour l'utilisateur, le rôle ou le groupe sélectionné.

Remarque :

- Analyseur d'accès est un produit du ServiceNow Store. Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique.
- L'analyseur d'accès emprunte l'identité de l'enregistrement d'identité pour récupérer les détails des autorisations et ne lit ni ne stocke aucune donnée personnelle ou sensible de l'identité.
- Les résultats de l'évaluation d'Access Analyzer sont les mêmes, quelles que soient les politiques d'accès définies pour les utilisateurs, telles que l'accès Zero Trust (ZTA). Les politiques ne sont évaluées que pendant la connexion réelle de l'utilisateur et ne sont pas évaluées pendant le flux de l'analyseur d'accès.
- L'analyseur d'accès ne permet pas d'évaluer avec précision l'accès aux ressources liées aux ressources du champ d'application géré et au développeur délégué.

Évaluer l'accès

L'évaluation de l'accès est une aptitude de l'analyseur ServiceNow d'accès qui aide les administrateurs à visualiser les autorisations pour l'utilisateur, le rôle ou le groupe sélectionné.

Il vous permet d'analyser et d'afficher les autorisations des utilisateurs, des groupes, des rôles pour une table, des includes de script pouvant être appelés par un client, des pages de l'interface utilisateur et des points de terminaison REST.

À l'aide d'Access Analyzer, les organisations peuvent améliorer leur posture de sécurité, leur gouvernance des identités, leur gestion des risques, atteindre leurs objectifs de conformité et comprendre qui (identité) a accès à quoi (ressources).

Comparer l'accès

L'accès de comparaison est une aptitude d'Access ServiceNow Analyzer V2 qui permet aux administrateurs de comparer l'accès des utilisateurs et de déterminer le niveau d'accès approprié pour les utilisateurs de votre ServiceNow instance.

Comparer l'accès peut être effectué entre les utilisateurs pour les enregistrements utilisateur et le contrôle d'accès.

Comparer l'accès vous permet d'effectuer l'analyse suivante :

- Niveau 1 : comparez les enregistrements des utilisateurs pour comprendre les attributs, les rôles et les groupes.
- Niveau 2 : comparez les contrôles d'accès pour exécuter l'analyse de la cause première en identifiant des problèmes d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantages

Voici quelques-uns des avantages de l'utilisation de l'analyseur d'accès :

- Analysez l'accès aux ressources (tables).
- Comparez l'accès de 2 utilisateurs.
- Comparez les rôles et les groupes de 2 utilisateurs.
- Générez un rapport indiquant si une identité a accès à une ressource (table).
- Identifiez qui a accès à l'hygiène de sécurité critique.
- Aide à prévenir la surallocation des autorisations.
- Respecter les principes de privilège minimum lors de l'implémentation des contrôles d'accès.
- Limitez l'accès à certaines données, notamment les applications, les tables, les lignes ou les colonnes et d'autres ressources.
- Fournir des options de génération de rapports pour les résultats de l'analyseur.
- Comparez l'accès entre les enregistrements utilisateur et les contrôles d'accès.
- Déterminez le niveau d'accès approprié pour les utilisateurs de votre ServiceNow instance.

Utilisation de l'analyseur d'accès

Analysez les identités et leur accès sur l'instance ServiceNow® .

Avant de commencer
Rôle requis : admin, access_analyzer_admin

La procédure suivante décrit les étapes d'accès à l'analyseur d'accès et d'utilisation des différentes fonctionnalités de l'analyseur d'accès.

Remarque :
Analyseur d'accès est un produit du ServiceNow® Store.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.

   L'analyseur d'accès est doté des capacités suivantes :

   - Évaluer l'accès
   - Comparer les enregistrements de l'utilisateur
   - Comparer les contrôles d'accès

2. Sélectionnez l'onglet respectif pour utiliser l'analyseur d'accès en fonction de vos besoins.

Utilisation de l'évaluation de l'accès

Analysez les identités sur l'instance ServiceNow® .

Avant de commencer
Rôle requis : admin, access_analyzer_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans la procédure suivante, nous vous expliquons les étapes d'accès à l'outil Évaluer l'accès dans l'analyseur d'accès et l'utilisation de ses différentes fonctionnalités.

Remarque :
Access Analyzer est un ServiceNow Store produit.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Évaluer l'accès** .
3. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse des accès et des autorisations

Champ	Description
Analyser par *	Analyser l'accès d'un utilisateur, d'un rôle ou d'un groupe
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

4. Spécifiez la description dans le champ **Description** .
5. **Sélectionnez Analyser les autorisations**.

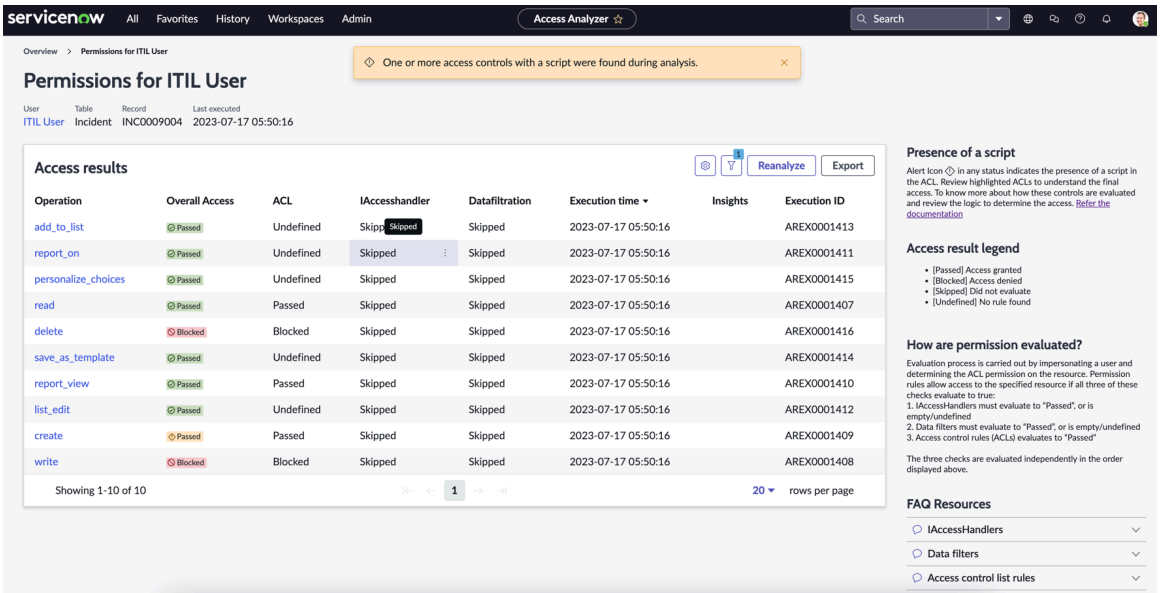
   Les résultats d'accès pour l'utilisateur s'affichent. De même, vous pouvez analyser les autorisations d'un groupe ou d'un rôle pour les types de règles suivants :

   - Table (enregistrement)
   - Les scripts d'appel client incluent
   - Points de terminaison REST

   Les résultats des accès s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La table Résultats d’accès comprend les champs suivants :

Résultats des accès

Champs	Description
Opération	Type d’opération que l’utilisateur, le groupe ou le rôle peut effectuer pour la table, l’enregistrement ou le champ sélectionné.
Accès global	Résultat de l’accès global. Les résultats sont les suivants : ○ [Réussi] Accès accordé ○ [Bloqué] Accès refusé ○ [Ignoré] N’a pas évalué ○ [Non défini] Aucune règle trouvée
ACL	Indique si une ACL est définie pour l’opération sélectionnée.
Gestionnaire d’accès	Une vérification interne du système à l’aide du code source masqué sur la plateforme. Le gestionnaire d’accès peut accorder ou refuser l’accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.
Filtration des données	Un filtre de données est une forme de contrôle d’accès conçu pour fonctionner avec les règles de contrôle d’accès (ACL) existantes sur votre instance.
Temps d'exécution	Heure à laquelle les résultats de l’accès ont été exécutés.
Aperçus	Plus d’informations sur l’opération sélectionnée.
ID d'exécution	ID unique pour chaque exécution de résultat d’accès.

6. Sélectionnez l’opération pour plus d’informations sur l’ACL.

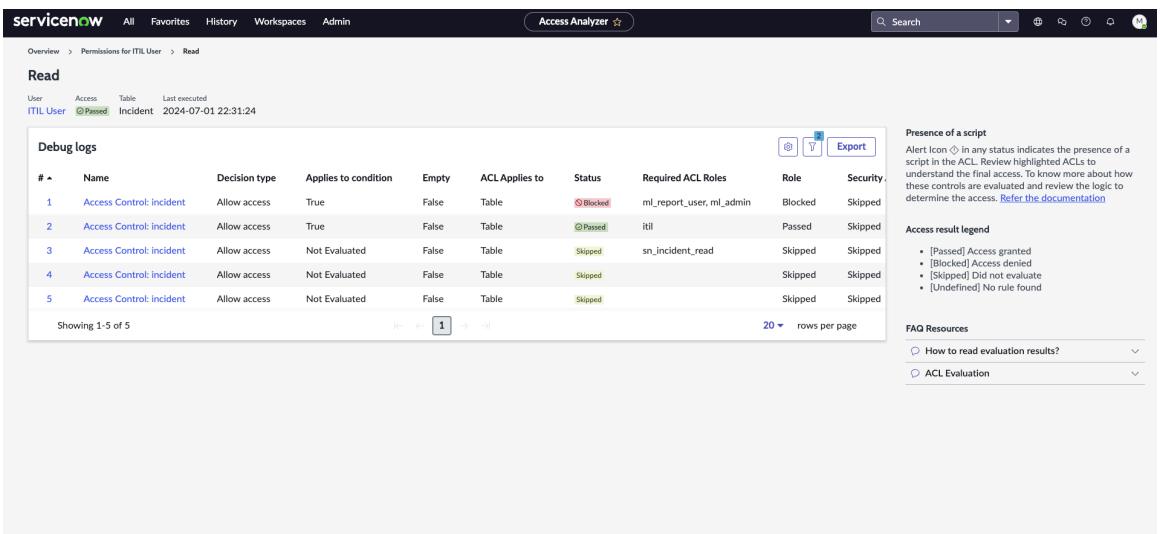
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, si vous sélectionnez **Lecture**, le contrôle d'accès associé à la lecture s'affiche.

Détails ACL

Champ	Description
Nom	Nom de l'ACL.
Type de décision	Type de décision configuré pour l'ACL. **Autoriser ou refuser l'accès**.
S'applique à la condition	Indique si l'ACL est appliquée à une condition.
ACL s'applique à	Détails sur la ressource à laquelle l'ACL est appliqué.
Statut	État du résultat de l'ACL ou de l'accès.
Rôles ACL requis	Détails du rôle requis pour accéder à la ressource.
Rôle	État du rôle. Réussi, ignoré ou bloqué.



Afficher les autorisations pour un utilisateur

Utilisez l'analyseur d'accès pour afficher les autorisations d'un utilisateur sélectionné.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un utilisateur sélectionné (**Utilisateur ITIL**) pour afficher les autorisations de la table **Incident** à l'aide de l'évaluation d'accès dans l'analyseur d'accès.

Remarque :
Analyseur d'accès est un produit du ServiceNow® Store.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

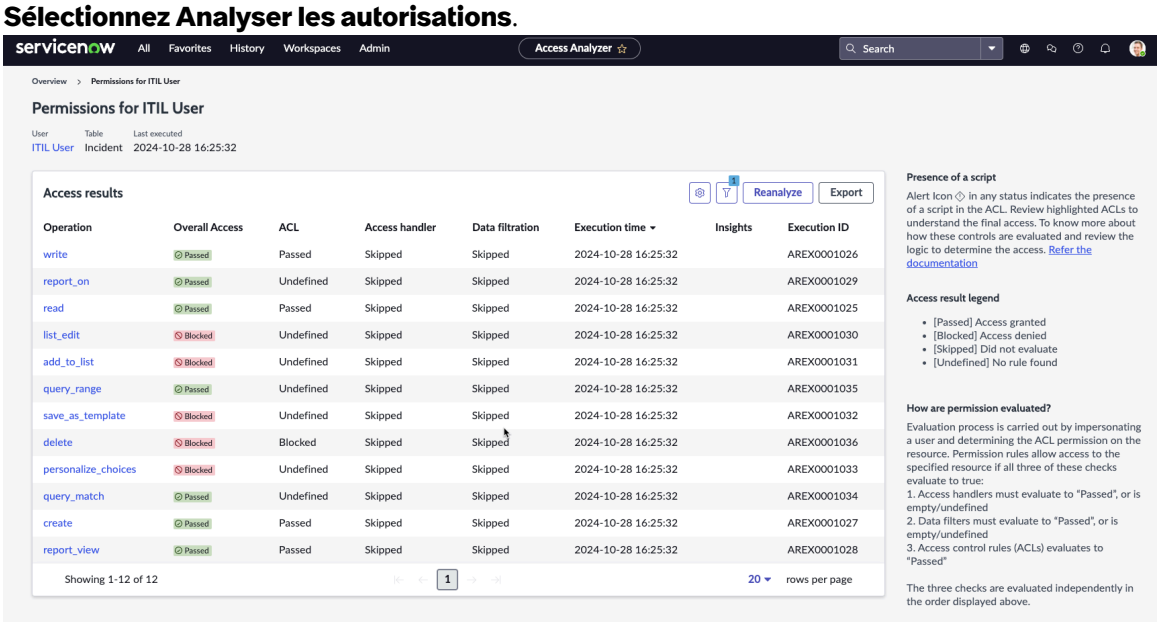
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez vos critères d'analyse des accès et des autorisations

Champ	Description
Analyser par *	Sélectionner **Utilisateur**.
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Utilisateur ITIL**.
Type de règle *	Analysez l'accès pour une **table**, une **page d'interface utilisateur**, un **point de terminaison REST** ou un **include de script de client pouvant être appelé**. Dans l'exemple, Table.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste. Dans cet exemple, **INC0000001**.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ peut être utilisé pour analyser l'autorisation même au niveau du champ. Par exemple, Actif, Créé par, etc.

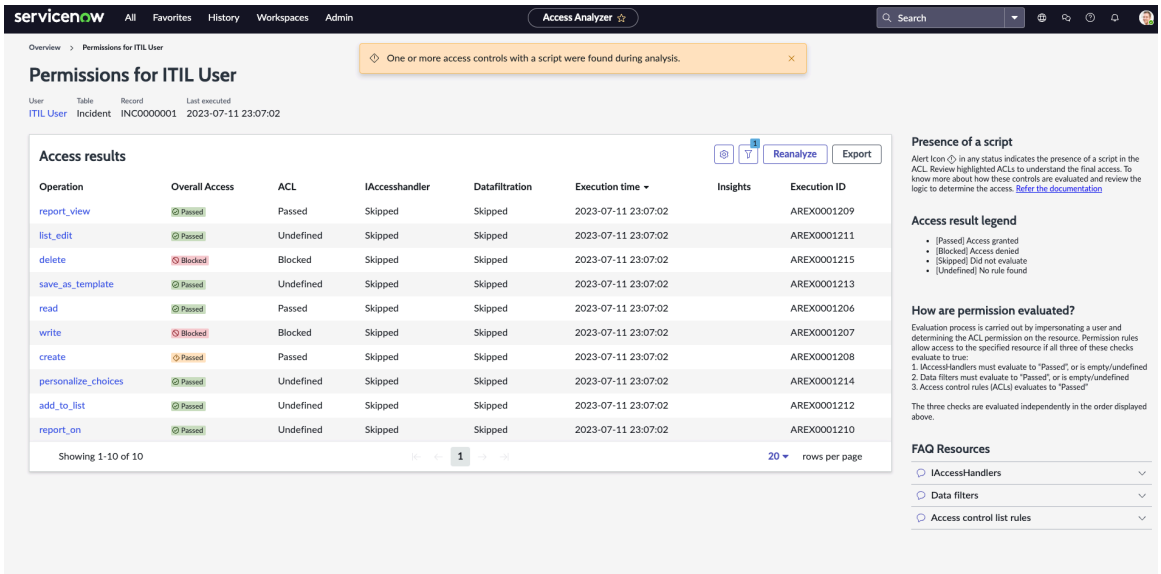
3. Spécifiez la description dans le champ **Description** .
4. **Sélectionnez Analyser les autorisations**.



Les **résultats d'accès** pour **l'utilisateur ITIL** s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), Gestionnaire d'accès et Données.

Prenons l'exemple de l'opération de **lecture** . Pour **l'utilisateur ITIL** , l'accès global est réussi, ce qui signifie que l'utilisateur est en mesure de lire l'enregistrement avec les autorisations appropriées (ACL).

De même, pour l'opération **de création** , l'accès global est transmis avec une icône d'alerte, ce qui signifie qu'il peut y avoir la présence d'un script pour l'évaluation de l'ACL.

Remarque :
Dans l'exemple, les opérations **d'écriture** et de **suppression** sont bloquées pour l'utilisateur sélectionné et l'utilisateur ne peut pas modifier ou supprimer l'enregistrement sélectionné (INC0000001).

5. Sélectionnez l'opération de lecture pour en savoir plus sur les journaux de débogage.



La page Journaux des débogages affiche la règle métier et les ACL associées nécessaires pour effectuer l'opération de **lecture** de l'enregistrement.

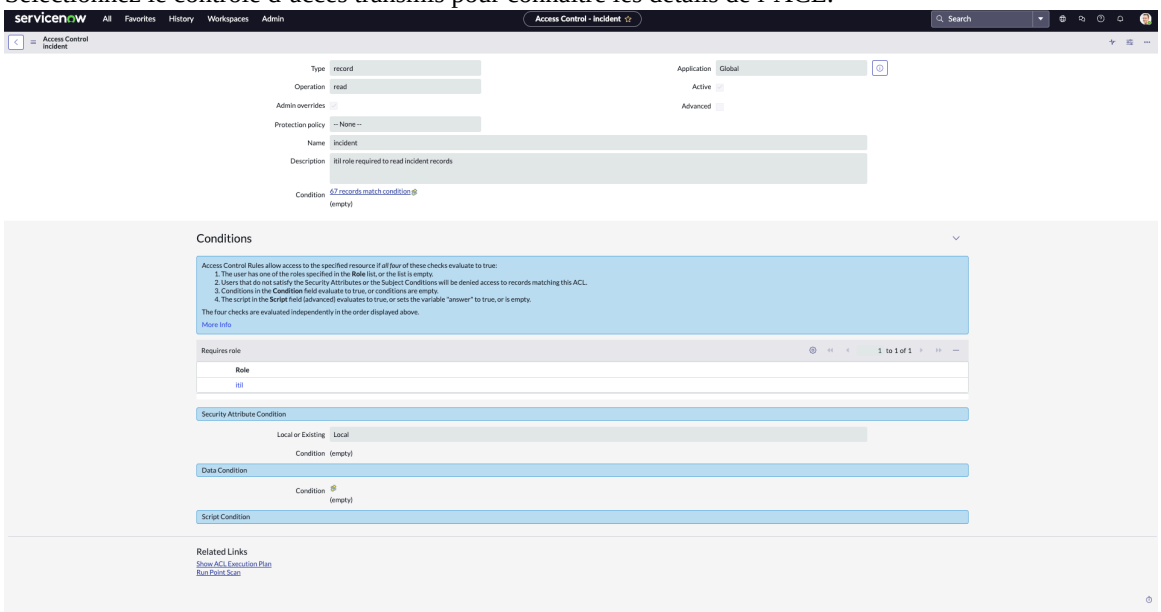
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les journaux des débogages montrent qu'il existe une règle métier et 4 ACL associées pour l'opération de lecture.

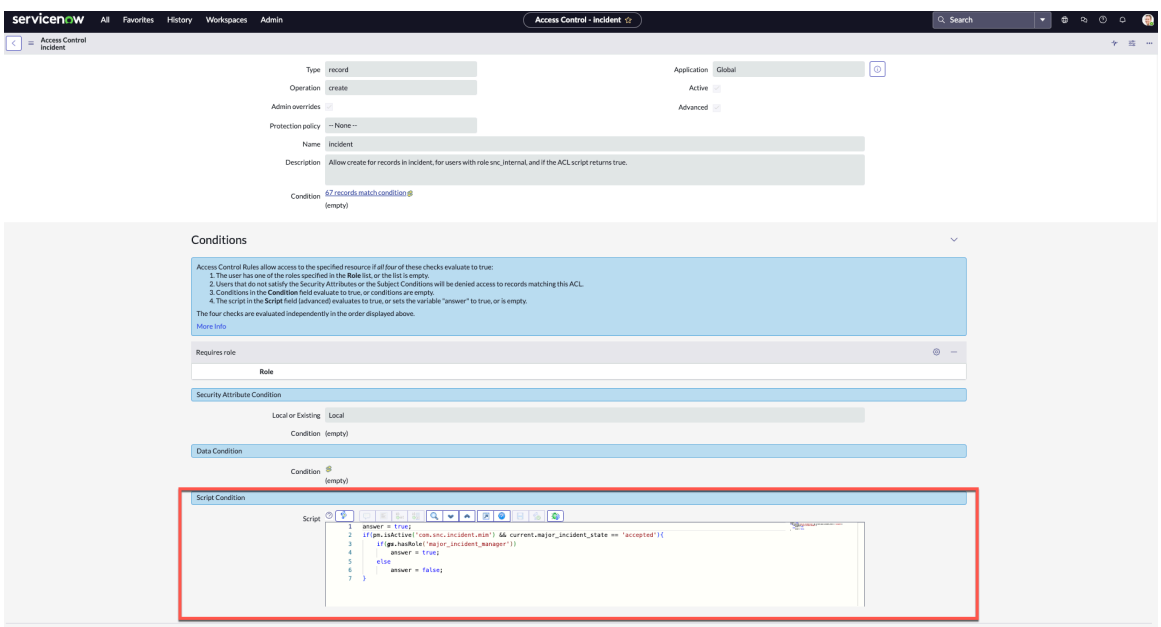
Il y a un statut **Réussi** pour l'une des ACL, ce qui signifie que pour lire l'enregistrement sélectionné, l'utilisateur dispose de l'ACL requise et peut lire l'enregistrement. Étant donné que l'une des ACL est **réussie**, les autres évaluations ACL sont **ignorées**.

6. Sélectionnez le contrôle d'accès transmis pour connaître les détails de l'ACL.



Les détails du contrôle d'accès pour l'ACL sélectionnée s'affichent.

Pour une opération sélectionnée avec la **fonction Réussi** et la présence d'un script. La page Contrôle d'accès affiche le script associé pour l'enregistrement.



Afficher les autorisations pour un rôle

Utilisez l'analyseur d'accès pour afficher les autorisations d'un rôle sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

La procédure suivante décrit les exemples d'étapes pour afficher les autorisations d'un rôle sélectionné (**user_admin**) pour afficher l'autorisation d'un point de terminaison d'API REST à l'aide de l'évaluation d'accès dans l'analyseur d'accès.

Remarque :
Analyseur d'accès est un produit du ServiceNow® Store.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

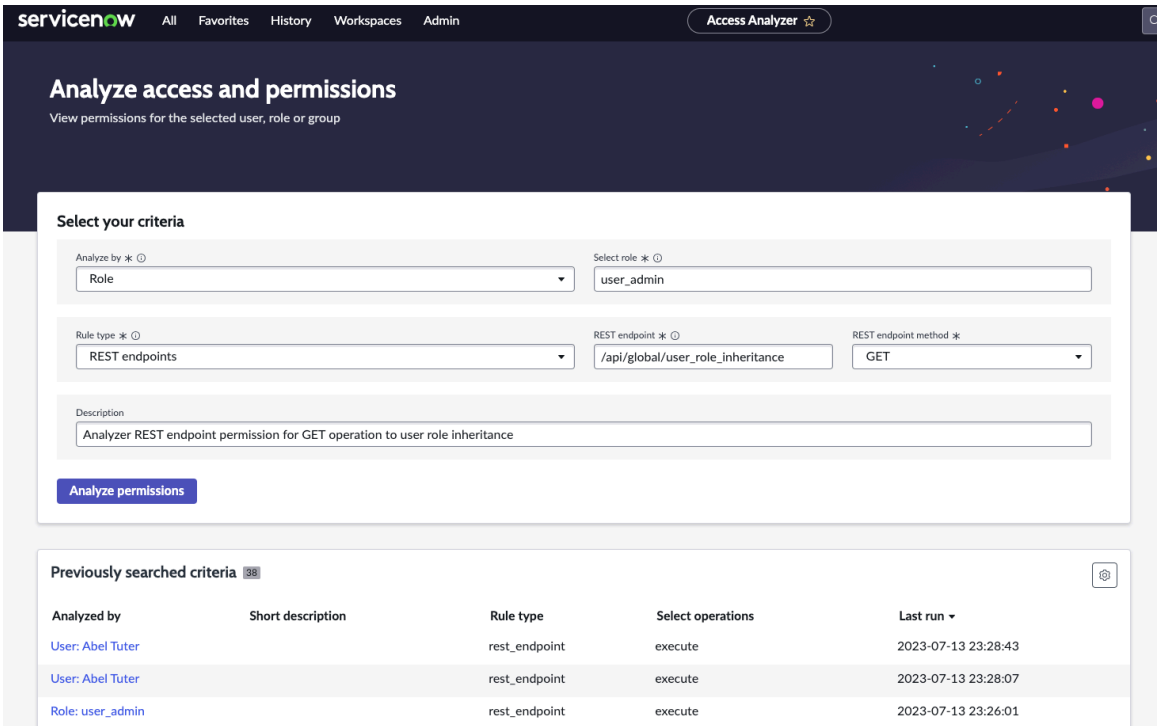
Sélectionnez vos critères d'analyse des accès et des autorisations

Champ	Description
Analyser par *	**Sélectionnez un rôle**.
Sélectionner un utilisateur *	Spécifiez un rôle à sélectionner dans la liste. Par exemple, **user_admin**.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé. Par exemple, **Point de terminaison REST**.
Point de terminaison REST*	Spécifiez un point de terminaison REST. Par exemple, `/api/global/user_role_inheritance`. **Remarque :** Le point de terminaison REST complet doit être utilisé lors de l'utilisation du champ sélectionné.
Méthode de point de terminaison REST *	Spécifiez une méthode de point de terminaison REST. Par exemple, GET.

3. Spécifiez la description dans le champ **Description** .
4. **Sélectionnez Analyser les autorisations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les **résultats d'accès** pour le rôle **user_admin** s'affichent.

Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), Gestionnaire d'accès et Données.

L'accès global pour le rôle est transmis, ce qui signifie que le rôle (**user_admin**) est en mesure d'accéder au **point de terminaison REST** pour la méthode **GET** sélectionnée.

Afficher les autorisations pour un groupe

Utilisez l'analyseur d'accès pour afficher les autorisations d'un groupe sélectionné.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

La procédure suivante décrit les exemples d'étapes pour afficher les autorisations d'un groupe sélectionné (**Gestion des incidents**) pour afficher les autorisations d'une page **d'interface utilisateur d'incident** à l'aide de l'évaluation de l'accès dans l'analyseur d'accès.

Remarque :
Analyseur d'accès est un produit du ServiceNow® Store.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse des accès et des autorisations

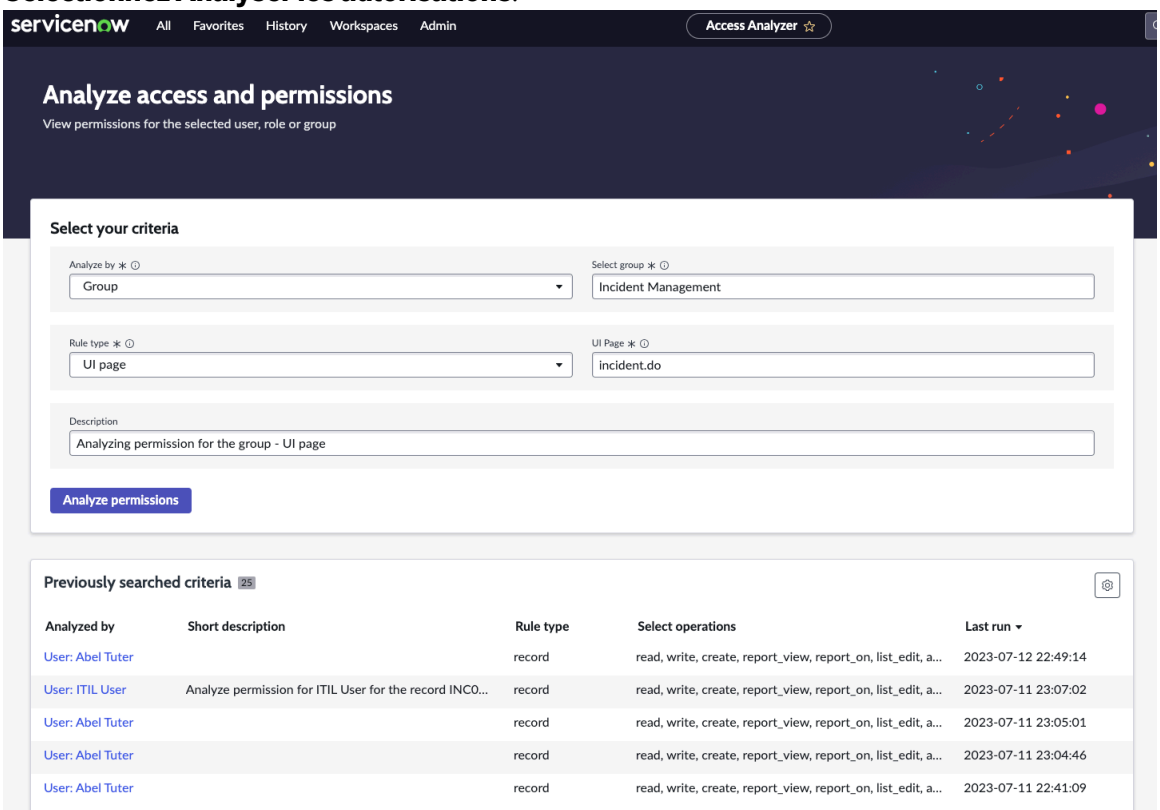
Champ	Description
Analyser par *	Sélectionnez **un groupe**.

Traduction automatique

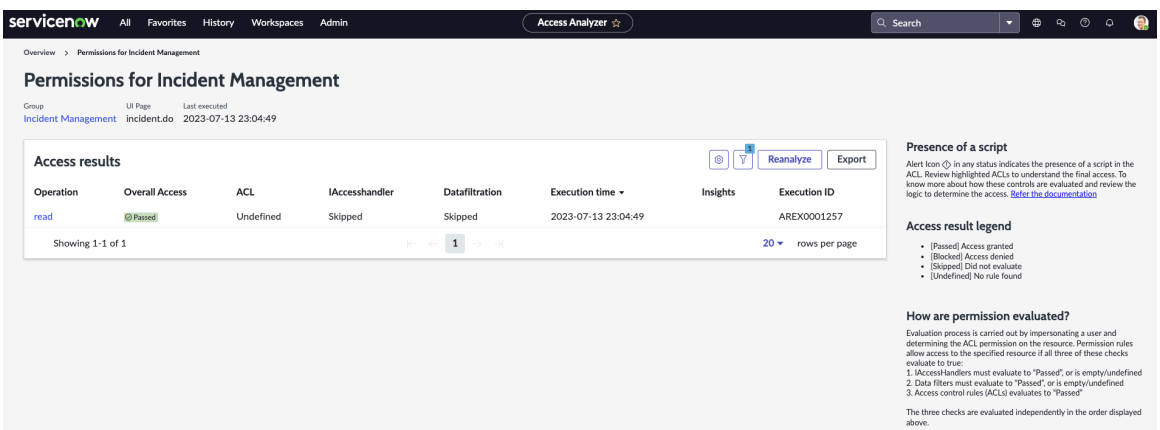
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d’utilisateur à sélectionner dans la liste. Par exemple, **Gestion des incidents**.
Type de règle *	Analysez l’accès pour une table, une page d’interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé. Par exemple, **page de l’interface utilisateur**.
Page de l’interface utilisateur *	Spécifiez la page de l’interface utilisateur. Par exemple, **incident.do**.

3. Spécifiez la description dans le champ **Description** .
4. **Sélectionnez Analyser les autorisations**.



Les **résultats d’accès** pour le groupe **Gestion des incidents** s’affichent.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), Gestionnaire d'accès et Données.

L'accès global du groupe est transmis, ce qui signifie que les utilisateurs du groupe (**Gestion des incidents**) peuvent accéder à l'enregistrement d'incident.

Exporter les requêtes d'analyseurs d'accès

Exportez les requêtes analysées à l'aide d'Access Analyzer.

Avant de commencer
Rôle requis : admin, access_analyzer_admin

La procédure suivante décrit les étapes d'accès à l'analyseur d'accès et d'utilisation des différentes fonctionnalités de l'analyseur d'accès.

Remarque :
Analyseur d'accès est un produit du ServiceNow® Store.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

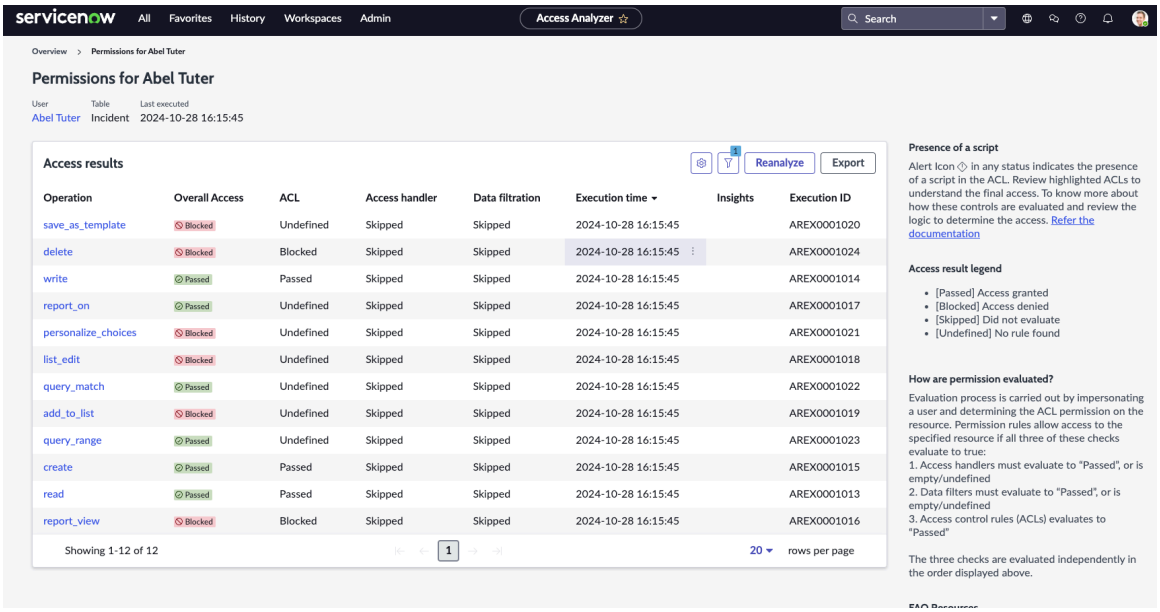
Sélectionnez vos critères d'analyse des accès et des autorisations

Champ	Description
Analyser par *	Analyser l'accès d'un utilisateur, d'un rôle ou d'un groupe
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

3. Spécifiez la description dans le champ **Description** .
4. **Sélectionnez Analyser les autorisations**.

Traduction automatique

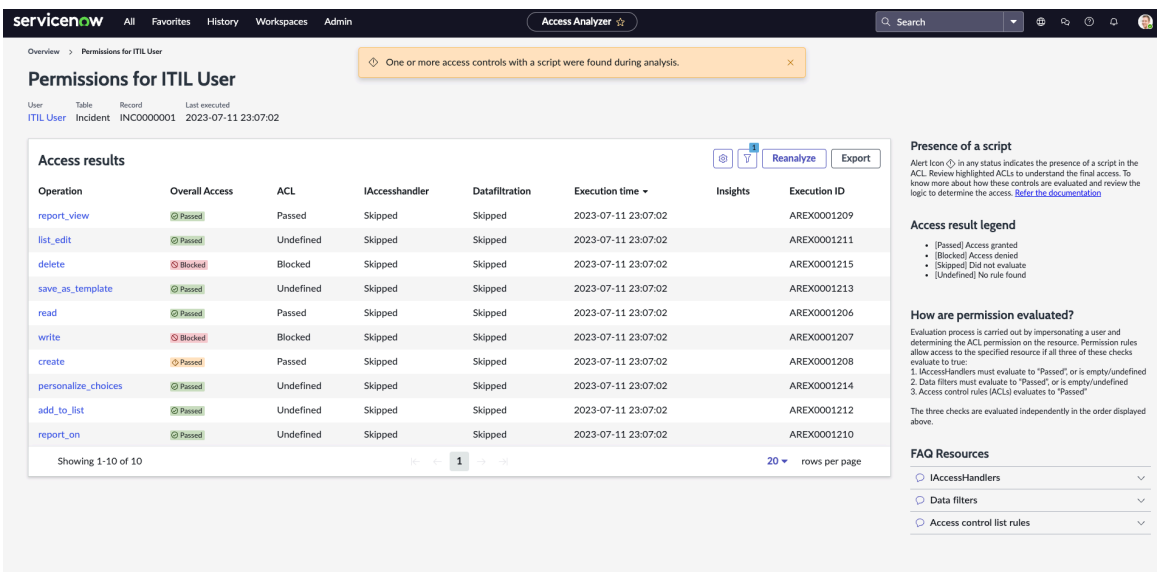
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats d'accès pour l'utilisateur s'affichent. De même, vous pouvez analyser les autorisations d'un groupe et d'un rôle pour les types de règles suivants :

- Table (enregistrement)
- Include de script Client pouvant être appelé
- Points de terminaison REST

Les **résultats d'accès** pour le type de règle sélectionné s'affichent.



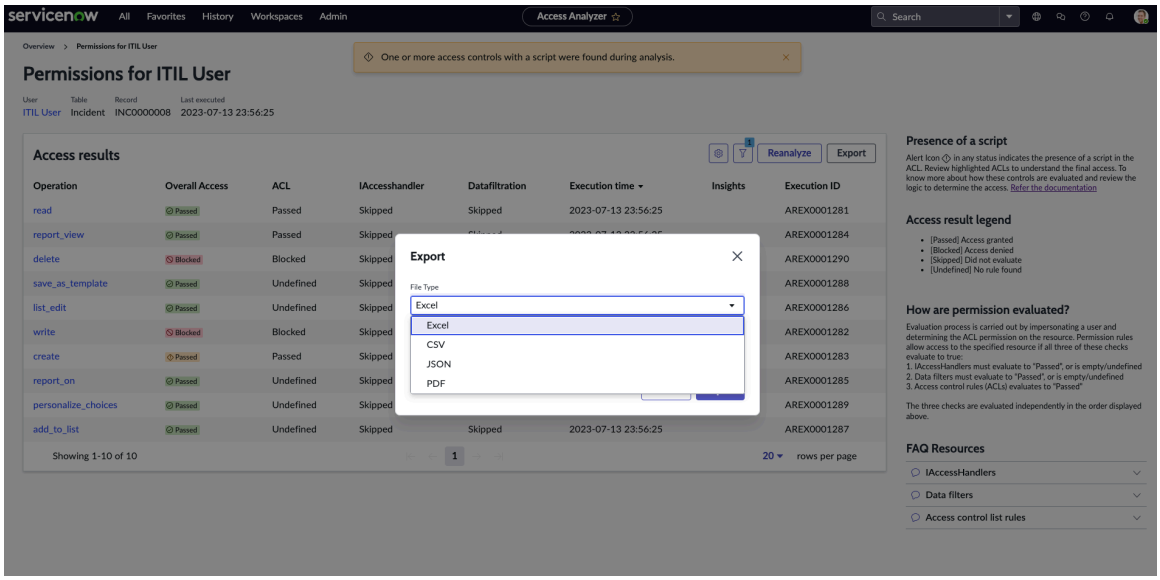
5. Cliquez sur **Exporter**.

a. Choisissez le type de fichier.

Les types de fichiers disponibles sont Excel, CSV, JSON, PDF.

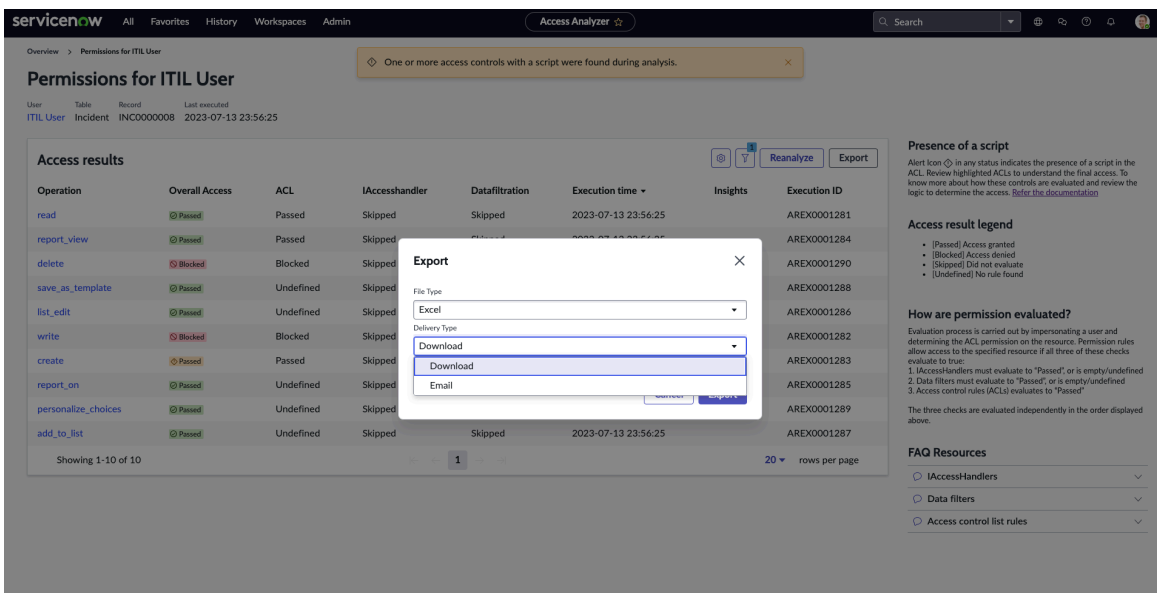
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



b. Choisissez le type de livraison.

Types de livraison disponibles comme Téléchargement et E-mail.



Comparaison des enregistrements de l'utilisateur

Comparez les enregistrements d'utilisateurs pour comprendre l'accès entre deux utilisateurs.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Dans la procédure suivante, nous vous expliquons les étapes de comparaison des enregistrements utilisateur à l'aide de l'analyseur d'accès.

Remarque :
Access Analyzer est un ServiceNow® Store produit.

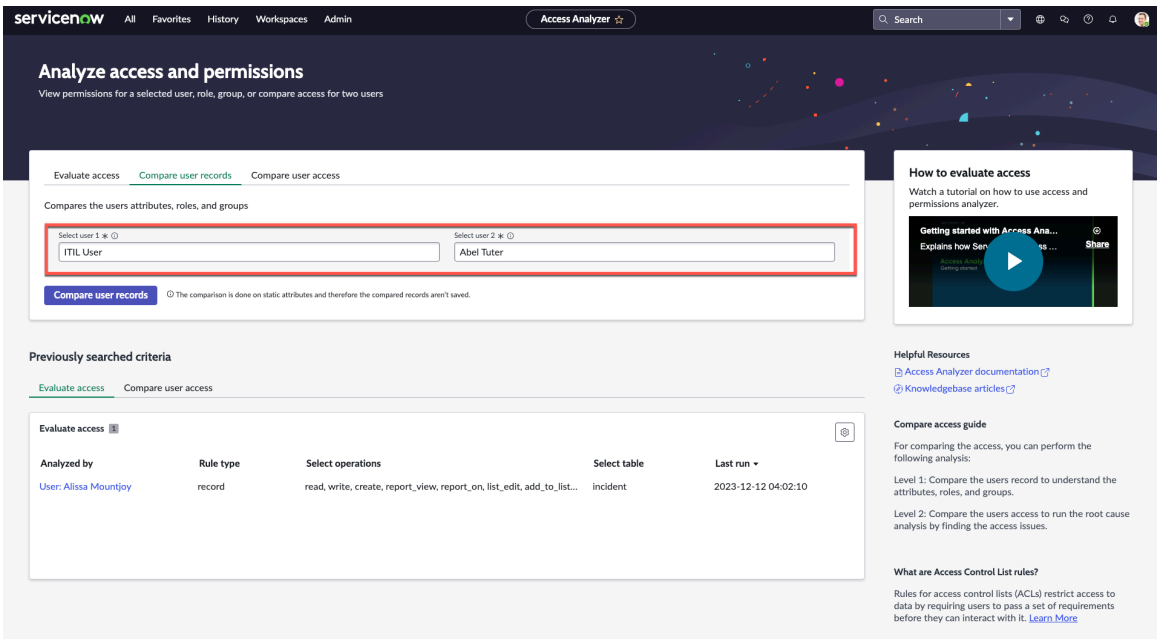
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Comparer les enregistrements de l'utilisateur** .
3. Sélectionnez **l'utilisateur 1** et **l'utilisateur 2** pour comparaison.

   Par exemple, Utilisateur ITIL en tant **qu'utilisateur 1** et Abel Tuter en tant **qu'utilisateur 2**.



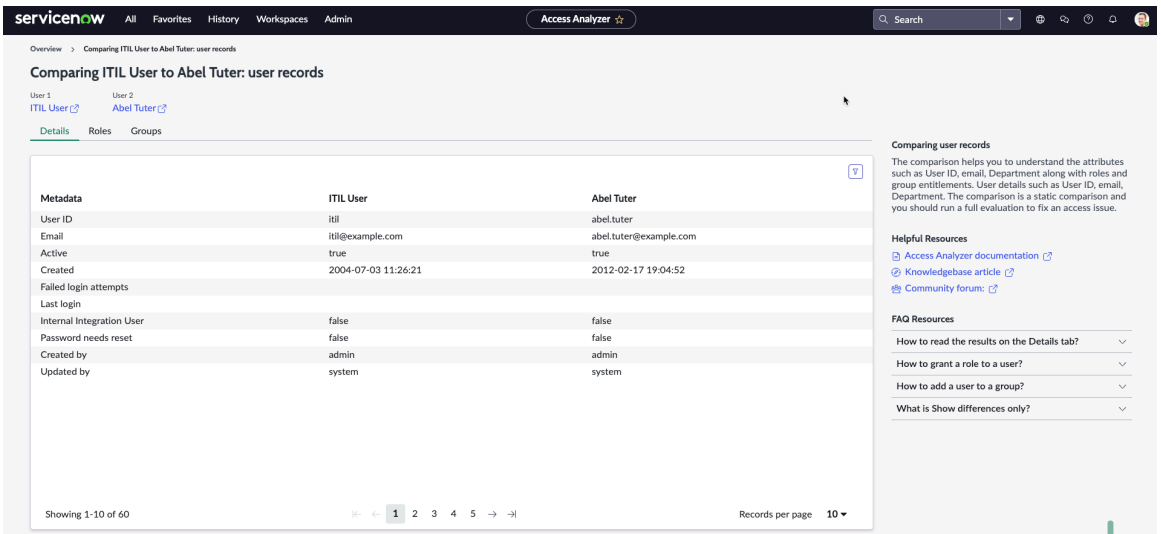
4. Sélectionnez **Comparer les enregistrements utilisateur**.

   Les résultats sont affichés avec les onglets suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Détails** : affichez les métadonnées de



l'utilisateur.

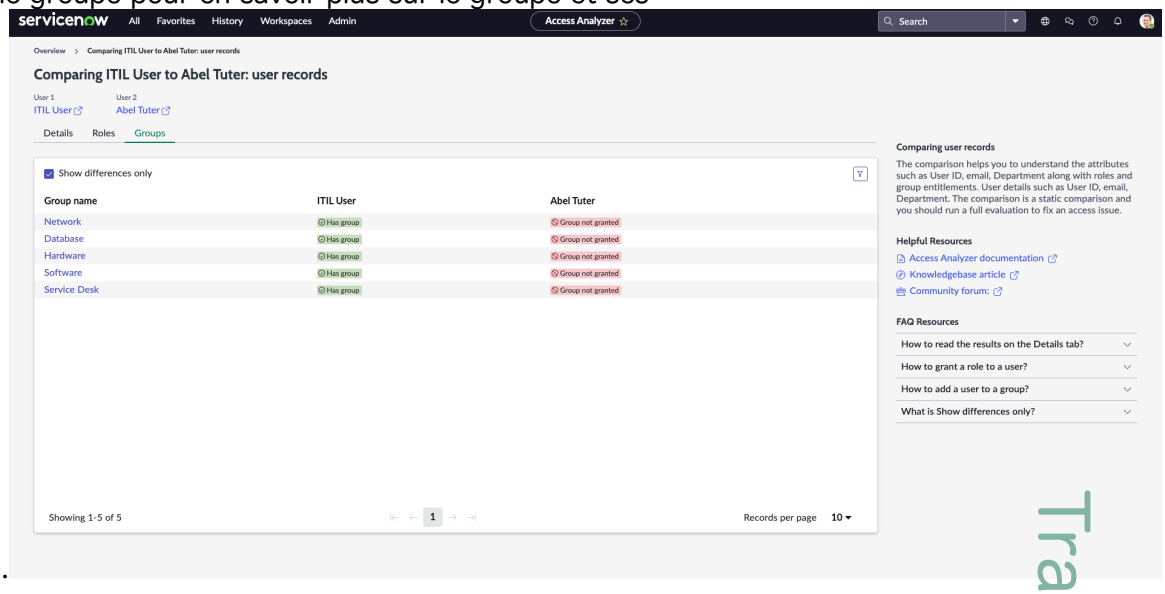
- **Rôles** : affiche les rôles affectés à l'utilisateur. Vous pouvez sélectionner le rôle pour en savoir plus sur le rôle et ses droits.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Groupes** : affichez les groupes affectés à l'utilisateur. Vous pouvez sélectionner le groupe pour en savoir plus sur le groupe et ses autorisations.



De même, vous pouvez comparer différents utilisateurs dans l'instance ServiceNow pour comprendre l'accès qui est affecté aux utilisateurs.

Comparaison de l'accès de l'utilisateur

Comparez le contrôle d'accès de l'utilisateur à l'aide de l'analyseur d'accès.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Dans la procédure suivante, nous vous expliquons comment comparer le contrôle d'accès entre les utilisateurs à l'aide de l'analyseur d'accès.

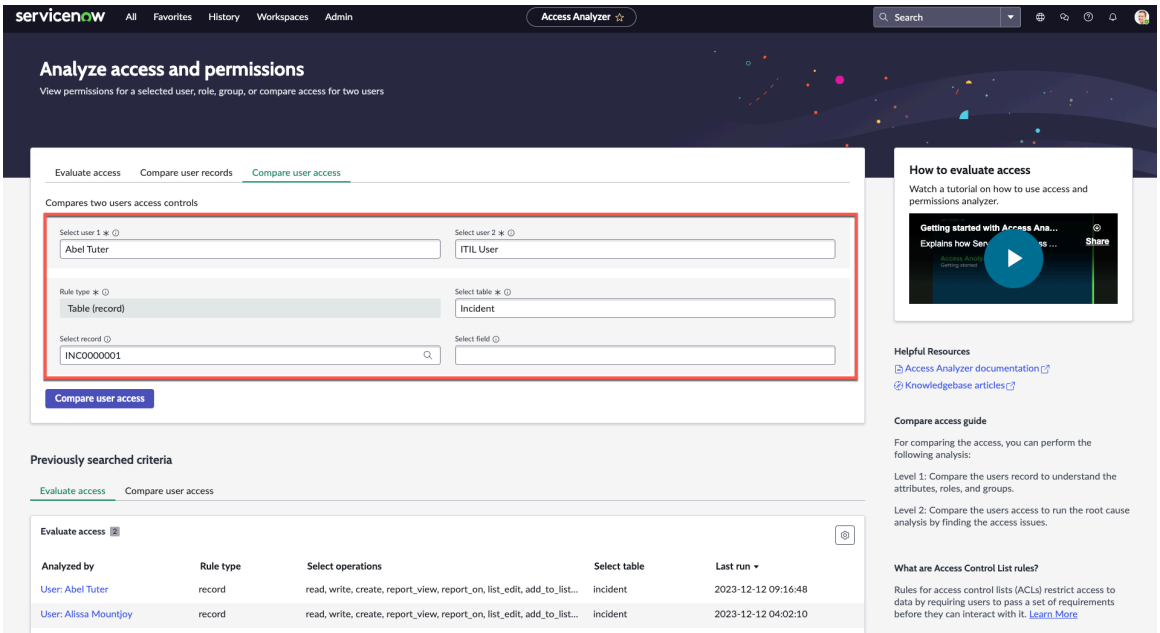
Remarque :
Access Analyzer est un ServiceNow® Store produit.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Comparer l'accès de l'utilisateur** .
3. Renseignez les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comparer l'accès de l'utilisateur

Champ	Description
Sélectionner l’utilisateur 1*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour comparaison.
Sélectionner l’utilisateur 2*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour le comparer à l’utilisateur 1.
Type de règle*	Analysez les autorisations d’accès pour une table. **Remarque :** Seules les autorisations d’accès à une table peuvent être utilisées dans **l’accès utilisateur de comparaison**.
Sélectionner une table*	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d’enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

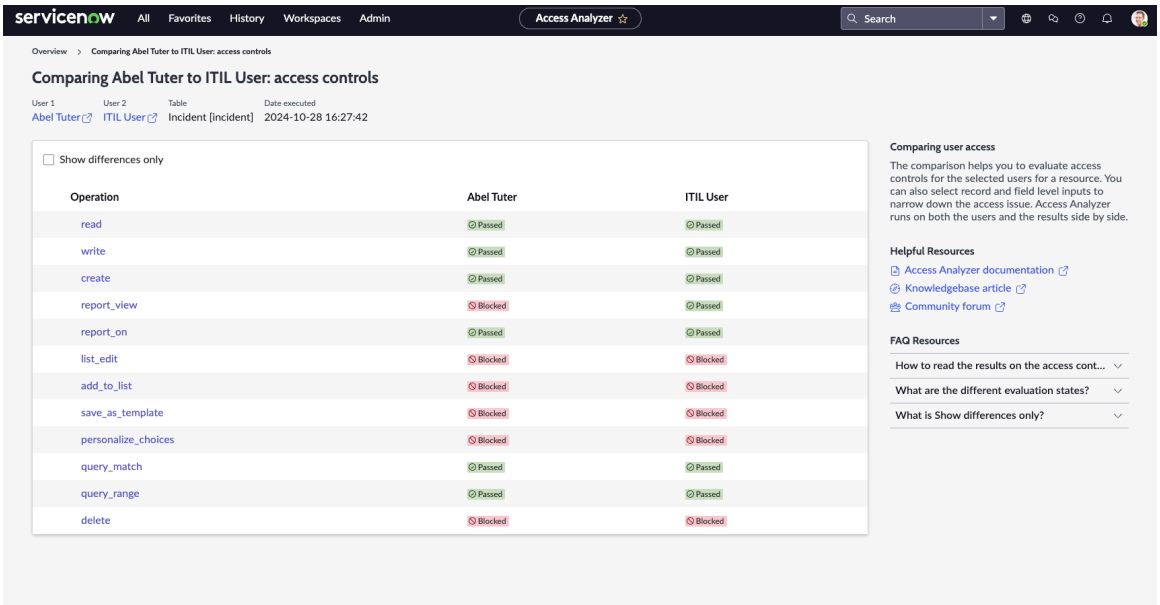
4. Sélectionnez **Comparer l’accès utilisateur**.

   Les résultats **de comparaison de l’accès utilisateur** pour les utilisateurs sélectionnés s’affichent.

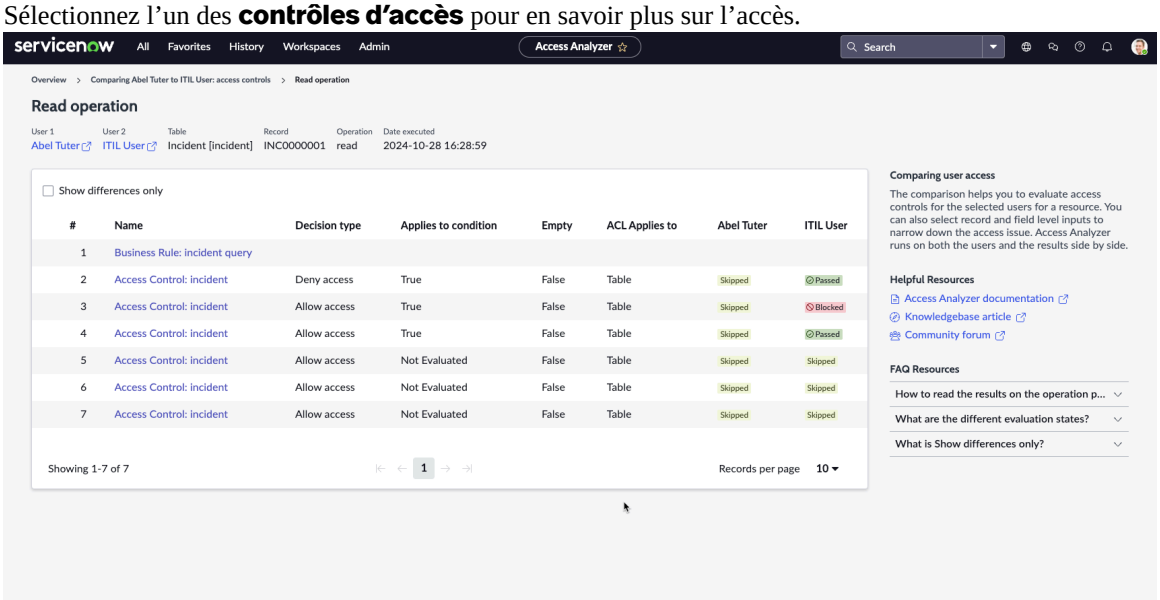
   La comparaison des résultats de l’accès utilisateur affiche l’opération et l’état d’évaluation de l’accès pour les utilisateurs. Par exemple, Abel Tuter et ITIL User.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



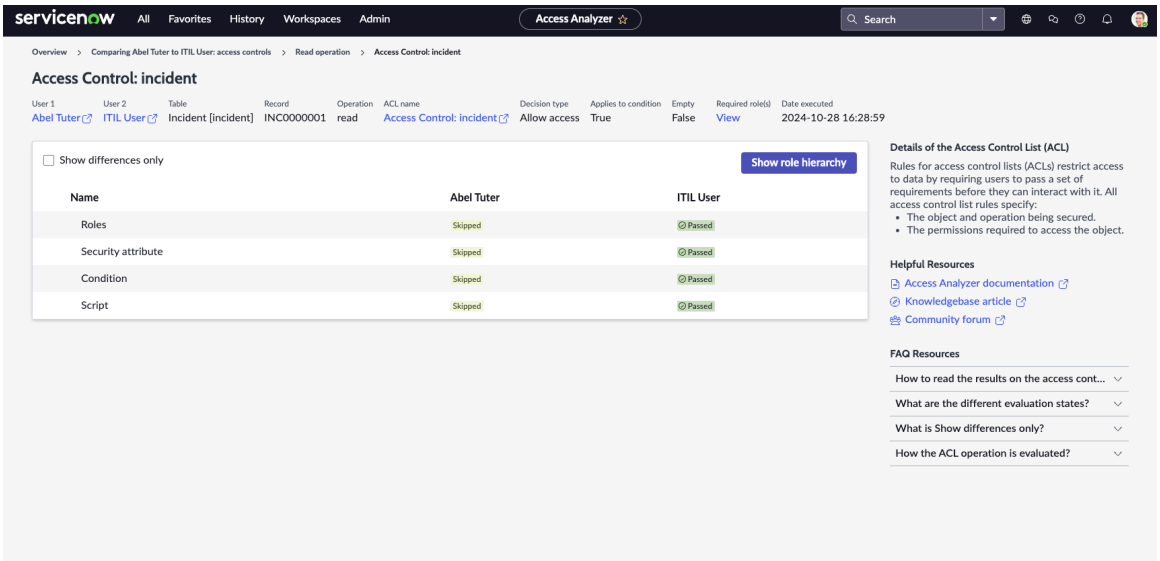
5. Sélectionnez l’opération pour en savoir plus sur l’évaluation des autorisations et les rôles affectés aux utilisateurs.
   Par exemple, **opération de lecture** .
6. Sélectionnez l’un des **contrôles d’accès** pour en savoir plus sur l’accès.



Les détails du contrôle d’accès tels que les rôles, l’attribut de sécurité, la condition et l’état d’évaluation du script sont affichés.

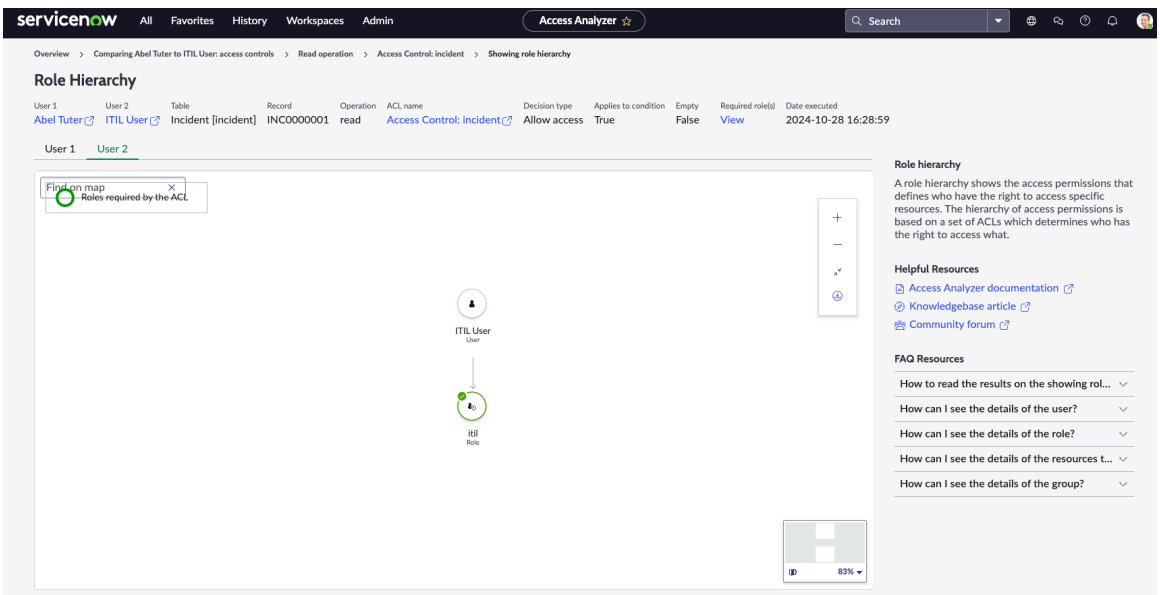
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Sélectionnez **Afficher la hiérarchie des rôles** pour en savoir plus sur les rôles et les groupes affectés à l'utilisateur et comparer les deux utilisateurs.

   En fonction de la hiérarchie des rôles, vous pouvez affecter les affectations de rôle et de groupe nécessaires à l'utilisateur pour avoir accès aux ressources (table).



   Dans l'exemple, **Abel Tuter** n'a pas d'itil affecté. Vous pouvez déterminer les affectations de rôle et de groupe nécessaires à l'utilisateur en examinant la hiérarchie des rôles.

   Vous pouvez sélectionner le nœud pour en savoir plus sur le rôle, les ressources auxquelles il peut accéder ou le groupe.

Affichage des critères précédemment recherchés dans l'analyseur d'accès

Affichez les critères recherchés précédemment dans l'analyseur d'accès.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Remarque :
Access Analyzer est un ServiceNow® Store produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

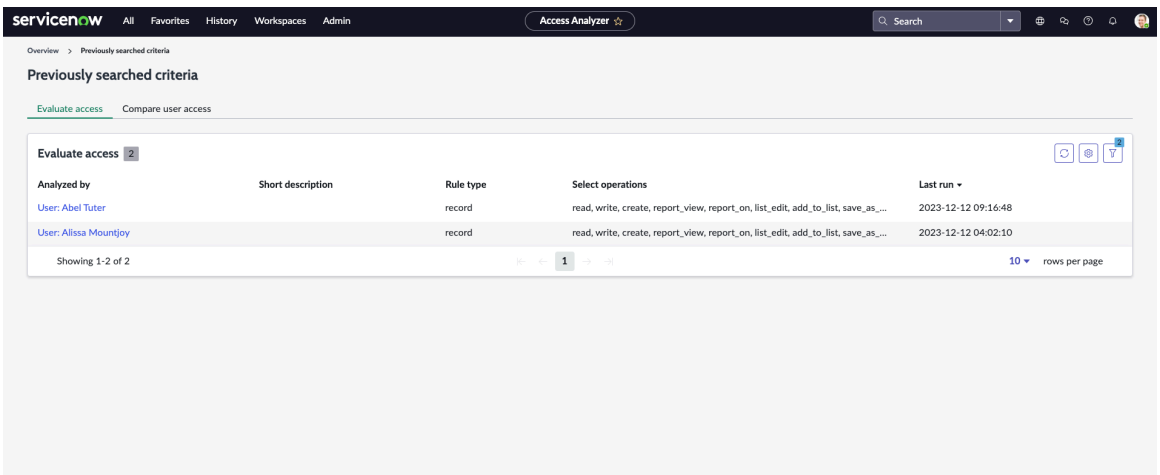
Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Requêtes d'analyseurs d'accès**.

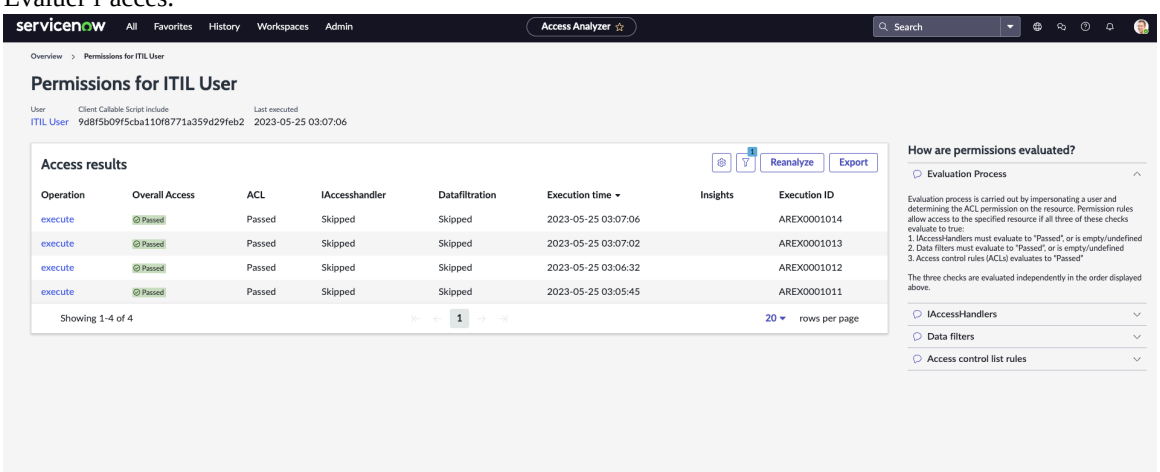
   Les critères recherchés précédemment comprennent les sections suivantes :

   - **Évaluer l'accès** : affiche les résultats basés sur les requêtes effectuées via les fonctionnalités **d'évaluation de l'accès** .
   - **Comparer l'accès de l'utilisateur** : affiche les résultats en fonction des requêtes effectuées via les fonctionnalités **Comparer l'accès de l'utilisateur** .

   Remarque :
   Les critères recherchés précédemment ne sont pas stockés lors de l'utilisation de la fonctionnalité Comparer les enregistrements de l'utilisateur.



2. Sélectionnez les liens **Analysé par** pour afficher les critères recherchés précédemment dans la section Évaluer l'accès.

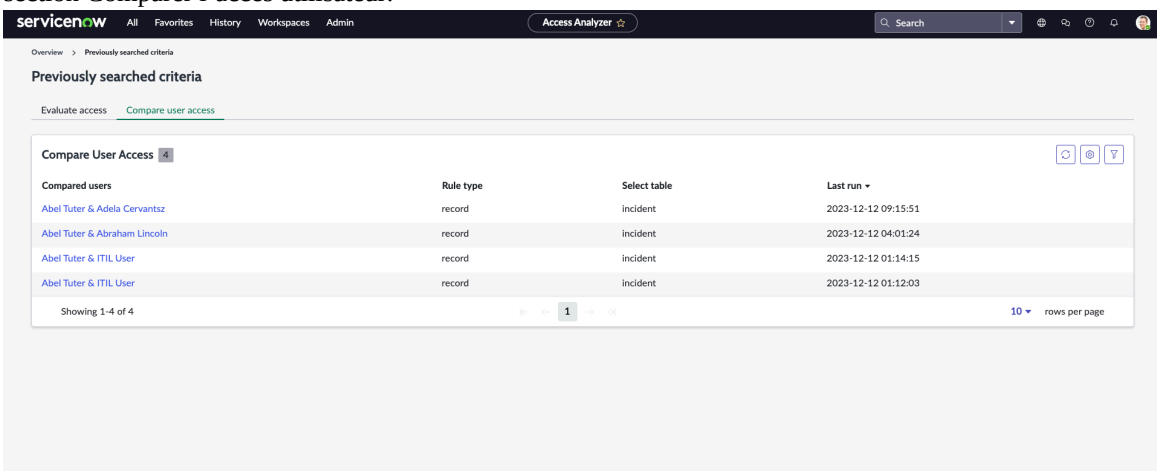


Vous pouvez sélectionner **Réanalyser** l'accès pour l'utilisateur. Exportez les détails à l'aide de l'option **Exporter** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez les liens **Utilisateurs comparés** pour afficher les critères recherchés précédemment dans la section Comparer l'accès utilisateur.



Évaluation de l'autorisation

Critères d'évaluation des autorisations lors de l'utilisation de l'analyseur d'accès.

Hiérarchie d'évaluation

L'autorisation pour l'utilisateur, le groupe ou le rôle sélectionné est évaluée dans la hiérarchie suivante :

- Règle métier : une règle métier est un script côté serveur qui s'exécute lorsqu'un enregistrement est affiché, inséré, mis à jour ou supprimé, ou lorsqu'une table est interrogée.
- Gestionnaire d'accès : vérification interne du système à l'aide du code source masqué sur la plateforme.
- Filtrage des données : le filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. Opération de lecture uniquement prise en charge par le filtre de données.
- Liste de contrôle d'accès (ACL) : les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Vous pouvez analyser l'accès et les autorisations de l'utilisateur, du rôle ou du groupe sélectionné à l'aide de l'analyseur d'accès. Les autorisations sont évaluées en fonction des types de règles suivants :

- **Évaluation au niveau** de la table : les ACL de rôle et d'attribut de sécurité sont utilisées pour l'évaluation au niveau de la table.
- **Évaluation au niveau de l'enregistrement ou du champ** : les ACL au niveau du rôle, de l'attribut de sécurité, de la condition et du script sont utilisées pour l'évaluation au niveau de l'enregistrement ou du champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Page de l'interface utilisateur** : prise en charge uniquement des opérations prêtes. Seules les ACL de niveau lecture sont évaluées.
- **Point de terminaison REST** : prise en charge uniquement de l'opération d'exécution. Seules les ACL de niveau d'exécution sont évaluées.

Les détails sur les champs importants dans les résultats d'accès sont les suivants :

- Présence d'un script
- Légende du résultat d'accès
- Processus d'évaluation
- Gestionnaires d'accès
- Filtres de données
- Règles de la liste de contrôle d'accès

Présence d'un script

Une icône d'alerte quel que soit l'état indique la présence d'un script dans l'ACL. Examinez les ACL en surbrillance pour comprendre l'accès final. Pour en savoir plus sur le mode d'évaluation de ces contrôles et sur la logique de détermination de l'accès, reportez-vous à la section Journaux de débogage d'analyseur d'accès.

Légende dans l'analyseur d'accès

Lors de l'analyse de l'accès et des autorisations, des légendes sont affichées dans le cadre du processus d'évaluation. Voici les légendes :

- [Réussi] Accès accordé
- [Bloqué] Accès refusé
- [Ignoré] N'a pas évalué
- [Non défini] Aucune règle trouvée

Processus d'évaluation

Le processus d'évaluation s'effectue en empruntant l'identité d'un utilisateur et en déterminant l'autorisation de la liste de contrôle d'accès (ACL) sur la ressource. Les règles d'autorisation activent l'accès à la ressource spécifiée si les vérifications suivantes sont évaluées comme vraies :

- Les gestionnaires d'accès doivent avoir la valeur « Réussi », ou sont vides ou non définis
- L'évaluation des filtres de données doit retourner la valeur « Réussi », ou est vide ou non définie
- Les règles de contrôle d'accès (ACL) sont évaluées comme « Réussi »

Gestionnaires d'accès

Une vérification interne du système à l'aide du code source masqué sur la plateforme. Le gestionnaire d'accès peut accorder ou refuser l'accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous ne pouvez pas modifier les vérifications du gestionnaire d'accès. Par exemple, une implémentation IAccessHandler est utilisée pour les vérifications d'accès sur les ressources d'application telles que l'accès en lecture.

Filtre de données

Le filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance.

Règles de la liste de contrôle d'accès

Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Forum aux questions

Forum Aux Questions lors de l'utilisation de l'analyseur d'accès.

Évaluer l'accès

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Évaluer l'accès dans l'analyseur d'accès :

Forum Aux Questions

Questions	Explication
Comment lire les résultats d'évaluation affichés par l'analyseur d'accès ?	Chaque ligne représente une liste de contrôle d'accès (ACL) individuelle. La séquence (#) dans les résultats, l'ordre dans lequel les ACL sont évaluées. L'état indique si l'accès global est accordé (réussi) ou refusé (bloqué).
Comment les ACL sont-elles évaluées ?	Au niveau d'une table, les ACL ne sont évalués que pour les rôles et les attributs de sécurité, les conditions et les scripts ne sont pas évalués. Les rôles sont évalués en premier. Si les rôles sont bloqués, les conditions et les scripts sont ignorés. Pour plus d'informations, consultez Configurer une règle ACL.
Quelles sont les légendes dans l'analyseur d'accès ?	Lors de l'analyse de l'accès et des autorisations, des légendes sont affichées dans le cadre du processus d'évaluation. Voici les légendes : • [Réussi] Accès accordé • [Bloqué] Accès refusé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions (suite)

Questions	Explication
	• [Ignoré] N'a pas évalué • [Non défini] Aucune règle trouvée
Que signifie l'icône d'alerte dans les résultats d'accès ?	Une icône d'alerte quel que soit l'état indique la présence d'un script dans l'ACL. Examinez les ACL en surbrillance pour comprendre l'accès final. Pour en savoir plus sur le mode d'évaluation de ces contrôles et sur la logique de détermination de l'accès, reportez-vous à la section Journaux de débogage d'analyseur d'accès.
Qu'est-ce que **IAccesshandler** ?	Une vérification interne du système à l'aide du code source masqué sur la plateforme. Il s'agit d'un contrôle de sécurité du système que vous ne pouvez pas modifier. **Le gestionnaire d'accès** peut accorder ou refuser l'accès à une ressource sans évaluer les ACL. Si ce **gestionnaire d'accès** est ignoré, les ACL sont évaluées. Vous ne pouvez en aucun cas modifier les vérifications du **gestionnaire d'accès** . Par exemple, une implémentation **IAccessHandler** est utilisée pour les contrôles d'accès sur les ressources d'application telles que l'accès en lecture seule.
Que sont les filtres de données ?	Les filtres de données sont une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance.
Qu'est-ce qu'une règle ACL ?	Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Affectations de rôles limitées dans le temps trouvées pour l'utilisateur en raison desquelles les résultats peuvent être affectés. Vous pouvez consulter les rôles à limite de temps affectés à l'utilisateur ici.

Comparer les enregistrements de l'utilisateur

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Comparer les enregistrements utilisateur dans l'analyseur d'accès :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions

Questions	Explication
Comment lire les résultats dans l'onglet Détails ?	L'onglet Détails affiche les métadonnées associées à l'utilisateur 1 et à l'utilisateur 2
Comment accorder un rôle à un utilisateur ?	Dans l'onglet Utilisateurs, vous pouvez vérifier le rôle qui doit être accordé à l'utilisateur et affecter ce rôle.
Comment ajouter un utilisateur à un groupe ?	Dans l'onglet Groupes, vous pouvez vérifier le groupe auquel l'utilisateur doit être ajouté et ajouter l'utilisateur au groupe.
Qu'est-ce que l'option Afficher uniquement la différence ?	Lorsque vous cochez la case Afficher uniquement les différences, seuls les rôles ou le groupe qui sont différents entre l'utilisateur 1 et l'utilisateur 2 s'affichent.

Comparer l'accès de l'utilisateur

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Comparer l'accès de l'utilisateur dans l'analyseur d'accès :

Forum Aux Questions

Questions	Explication
Comment lire les résultats sur la page de comparaison de contrôle d'accès ?	La page de comparaison des contrôles d'accès affiche les états d'évaluation pour différentes opérations ACL.
Quels sont les différents états d'évaluation ?	Lorsque l'on compare les contrôles d'accès entre les utilisateurs, les différents états d'évaluation sont les suivants : • Réussi • Bloqué
Qu'est-ce que l'option Afficher uniquement les différences ?	Lorsque vous cochez la case Afficher uniquement les différences, seul l'état d'évaluation de l'opération qui est différent entre l'utilisateur 1 et l'utilisateur 2 s'affiche.
Comment l'opération ACL est-elle évaluée ?	La liste de contrôle d'accès (ACL) est la règle pour les listes de contrôle d'accès qui restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée : • Rôle • Attribut de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions (suite)

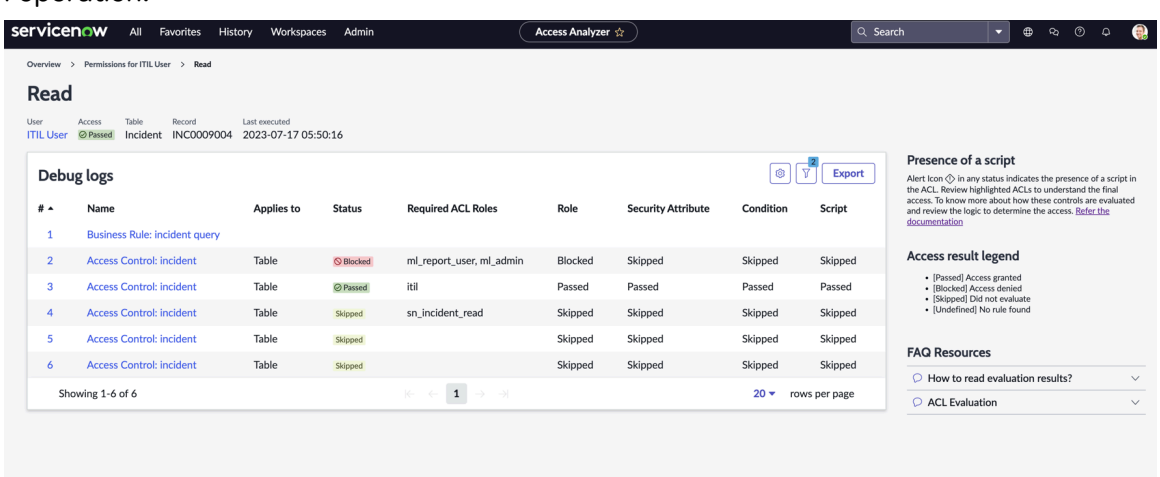
Questions	Explication
	• Condition • Script
Comment lire les résultats sur la page d'affichage de la hiérarchie des rôles ?	La page d'affichage de la hiérarchie des rôles affiche le rôle affecté à l'utilisateur 1 et à l'utilisateur 2. Vous pouvez comprendre le rôle requis pour l'utilisateur pour une opération ACL particulière.
Comment puis-je voir les détails de l'utilisateur ?	Vous pouvez sélectionner l'icône **Utilisateur (nœud)** > **Actions supplémentaires** > **Afficher l'utilisateur** détails pour en savoir plus sur l'utilisateur.
Comment puis-je voir les détails du rôle ?	Vous pouvez sélectionner l'icône **Rôle (nœud)** > **Actions supplémentaires** > **Afficher le rôle** détails pour en savoir plus sur le rôle.
Comment puis-je voir les détails des ressources auxquelles le rôle peut accéder ?	Vous pouvez sélectionner l'icône **Rôle (nœud)** > **Actions supplémentaires** > **Afficher toutes les ressources auxquelles le rôle a accès** pour connaître les ressources auxquelles le rôle peut accéder.
Comment puis-je voir les détails du groupe ?	Vous pouvez sélectionner l'icône **Groupe (nœud)** > **Actions supplémentaires** > **Afficher le groupe** détails pour en savoir plus sur le groupe.

Journaux de débogage d'analyseur d'accès

Les journaux des débogages affichent les détails de l'opération de sélection du résultat de l'accès.

Champs dans les journaux des débogages

Les journaux de débogage de l'analyseur d'accès affichent des informations sur l'opération sélectionnée pour comprendre les autorisations, les règles métier et les ACL associées à l'opération.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les champs et leur description dans les journaux de débogage sont les suivants :

Journaux des débogages

Champs	Description
Nom	Les détails de la règle métier ou de l'ACL. Vous pouvez sélectionner la règle métier d'ACL pour plus d'informations.
Concerne	Détails de l'application d'ACL au niveau d'un champ, d'un enregistrement ou d'une table.
Statut	État de l'ACL pour le rôle et l'autorisation associés.
Requiert une ACL	Rôle requis pour accéder au champ, à l'enregistrement ou à la table.
Rôle	Les détails sur le rôle en cours Bloqué, Réussi, Ignoré pour le contrôle d'accès.
Attribut de sécurité	Les détails sur l'attribut de sécurité en cours Bloqué, Réussi, Ignoré pour le contrôle d'accès.
Condition	Le détail de la condition bloquée, réussie, ignorée pour le contrôle d'accès.
Script	Les détails du script bloqué, transmis ou ignoré pour le contrôle d'accès.
Personnalisé	Les détails de l'ACL personnalisée, le cas échéant, pour le contrôle d'accès.
Application	État de l'application. Global ou Store.

Hiérarchie d'évaluation

L'autorisation pour l'utilisateur, le groupe ou le rôle sélectionné est évaluée dans la hiérarchie suivante :

- Règle métier : une règle métier est un script côté serveur qui s'exécute lorsqu'un enregistrement est affiché, inséré, mis à jour ou supprimé, ou lorsqu'une table est interrogée.
- Gestionnaire d'accès : vérification interne du système à l'aide du code source masqué sur la plateforme.
- Filtrage des données : un filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. Les filtres de données ne prennent en charge que l'opération de lecture.
- Liste de contrôle d'accès (ACL) : les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation de la liste de contrôle d'accès

Les ACL pour les opérations sont évaluées dans la séquence comme suit :

- Rôle
- Attribut de sécurité
- Condition
- Script

Présence d'un script

Une icône d'alerte quel que soit l'état indique la présence d'un script dans l'ACL. Examinez les ACL en surbrillance pour comprendre l'accès final.

Remarque :
Lors d'une requête d'analyseur d'accès, les règles métier sont exécutées en premier, puis la liste de contrôle d'accès.

Séquence d'exécution

La séquence d'exécution des résultats d'accès dans différents scénarios est la suivante :

- **Présence d'une ACL héritée ou d'un caractère générique** : au cours de la séquence d'exécution, les ACL héritées sont évaluées en premier, puis les ACL génériques.
- **Une ACL est transmise, les autres sont ignorées** : pendant l'exécution et l'évaluation de l'autorisation, si une ACL est transmise, l'exécution et l'évaluation de l'autre ACL sont ignorées. Parce que l'autorisation globale pour l'opération sélectionnée nécessite une ACL pour accéder à un champ, un enregistrement ou une table d'une identité.
- **Exécution des ACL au niveau du champ et au niveau de la table** : pendant l'exécution, les ACL au niveau du champ sont exécutées en premier, suivies par les ACL au niveau de la table pour fournir des résultats plus granulaires lors de l'analyse de l'accès d'une identité.
- **Évaluation en présence d'une ACL scriptée** : en présence d'un script, l'accès global à l'opération est transmis avec une icône d'alerte pour indiquer le script dans l'ACL.

Simulateur d'accès

Le simulateur d'accès vous permet de simuler le changement de l'accès à la table spécifiée une fois qu'un rôle ou un groupe est affecté ou supprimé de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Access Simulator.

Utiliser



Comprendre comment utiliser le simulateur d’accès.

Configurer



Savoir comment configurer le simulateur d’accès.

Forum Aux Questions



Obtenez des détails sur les questions fréquemment posées sur le simulateur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découverte du simulateur d'accès

Le simulateur d'accès vous permet de simuler le changement de l'accès à la table spécifiée une fois qu'un rôle ou un groupe est affecté ou supprimé de l'utilisateur.

Les administrateurs peuvent utiliser le simulateur d'accès pour simuler les besoins d'accès de leurs utilisateurs sur une table spécifiée et comprendre comment les contrôles d'accès changent pour un utilisateur. Cela aide à comprendre rapidement l'accès actuel des utilisateurs et à comprendre les impacts de l'attribution ou de la suppression de rôles aux utilisateurs.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

Le simulateur d'accès peut être utilisé pour simuler l'accès sur un utilisateur dans les cas suivants :

- Ajout de rôles aux utilisateurs
- Suppression des rôles des utilisateurs
- Ajout d'utilisateurs à des groupes
- Suppression des utilisateurs des groupes

Pour en savoir plus sur les paramètres du simulateur d'accès et l'activation des actions, reportez-vous à la section Configuration du simulateur d'accès (Prendre des mesures).

Configuration du simulateur d'accès (Prendre des mesures)

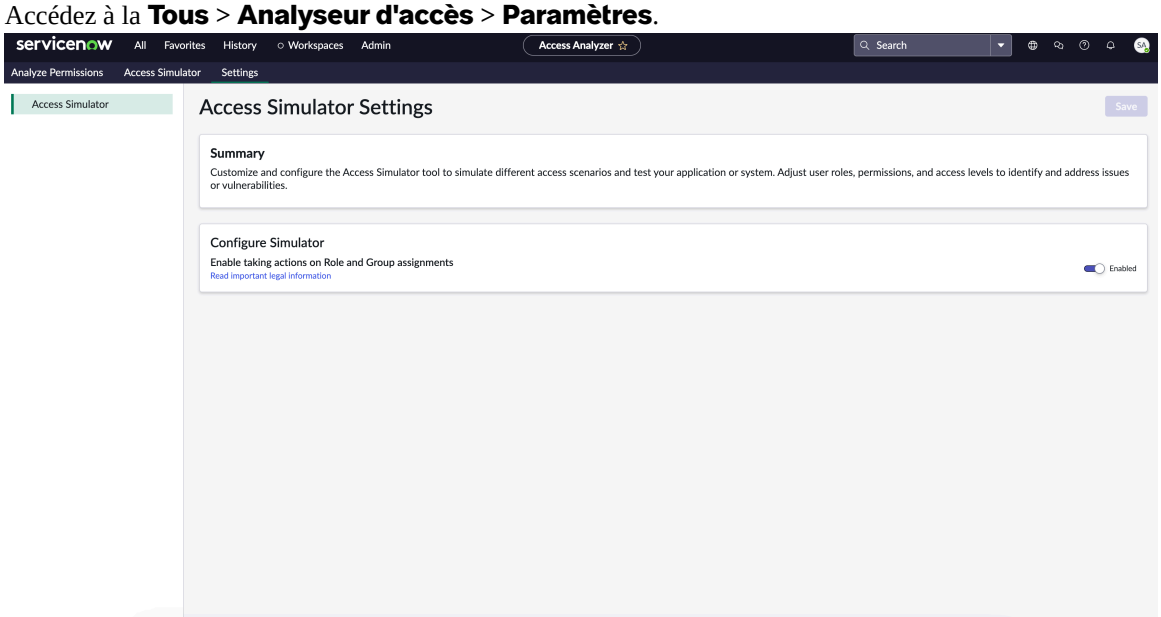
Configurez les options Prendre des mesures pour terminer les affectations de rôle et de groupe que vous souhaitez ajouter après la simulation.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Paramètres**.



2. Sélectionnez le commutateur à activer.
   Lisez les informations légales avant d'activer le simulateur d'accès (Prendre des mesures).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Accepter**.
4. Sélectionnez **Enregistrer** pour enregistrer la configuration.

Utilisation du simulateur d'accès

Utilisez le simulateur d'accès pour simuler le changement de l'accès de l'utilisateur à la table spécifiée une fois qu'un rôle ou un groupe est affecté ou supprimé.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Activez l'option Prendre des mesures. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez l'option **Simuler** sous chaque section en fonction des scénarios suivants :
   - Ajout de rôles aux utilisateurs
   - Suppression des rôles des utilisateurs
   - Ajout d'utilisateurs à des groupes
   - Suppression des utilisateurs des groupes

Ajout de rôles aux utilisateurs

Utilisez le **rôle Simuler Ajouter pour simuler** les changements d'accès de l'utilisateur pour une ressource (tables).

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Activez l'option Prendre des mesures. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Ajouter un rôle à l'utilisateur.
3. Spécifiez les champs suivants pour vos critères de simulation :

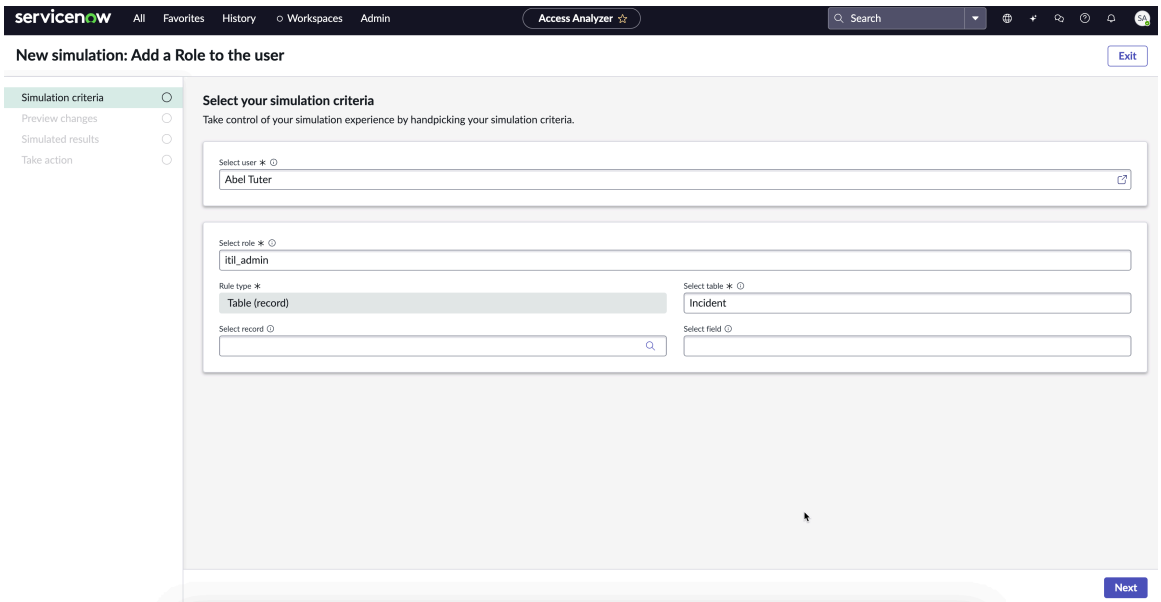
Ajouter un rôle à l'utilisateur

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un rôle *	Spécifiez un rôle à sélectionner dans la liste. Dans cet exemple, **itil_admin**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.

Traduction automatique

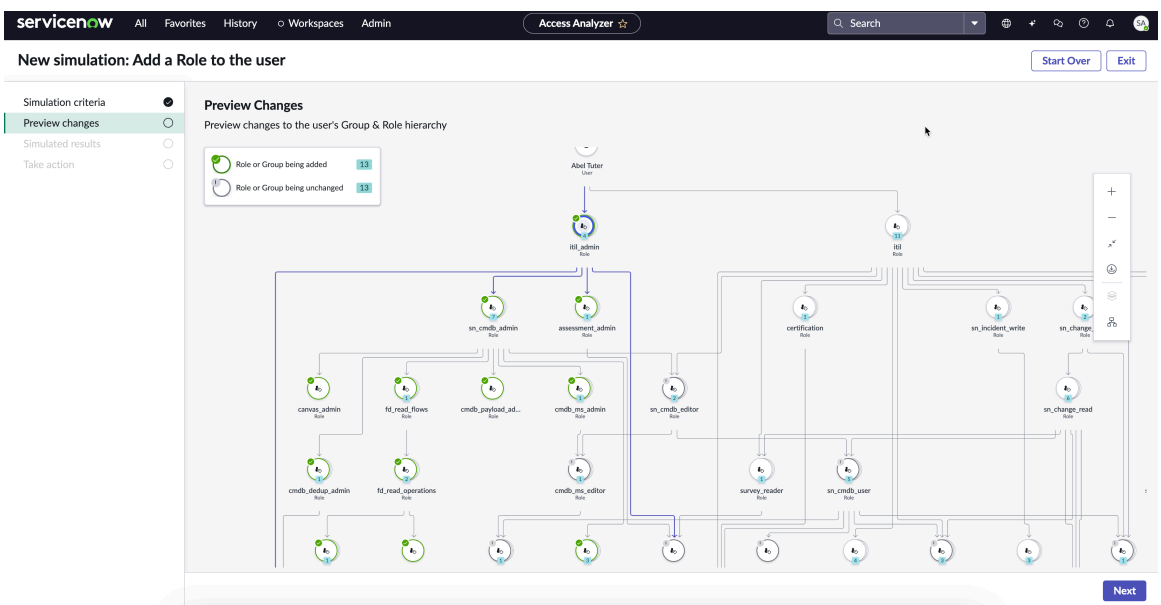
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste (facultatif).
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ peut être utilisé pour analyser l'autorisation même au niveau du champ. Par exemple, Actif, Créé par, etc.



4. Sélectionnez **Suivant**.

5. Prévisualisez les modifications.
   Les rôles nouvellement affectés sont simulés dans les changements de préversion. Vous pouvez valider les rôles et les rôles enfants qui sont ajoutés à l'utilisateur avant de passer à l'étape suivante.

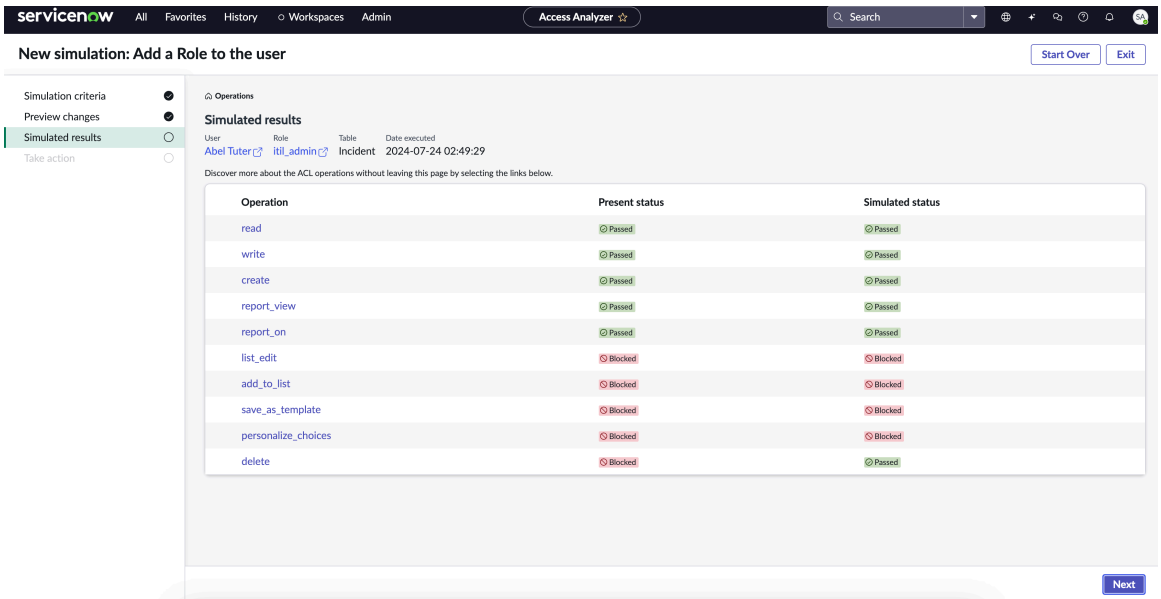


Vous pouvez voir les nouveaux rôles qui sont ajoutés dans le cadre de **itil_admin** rôle s'affiche avec les rôles existants de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.

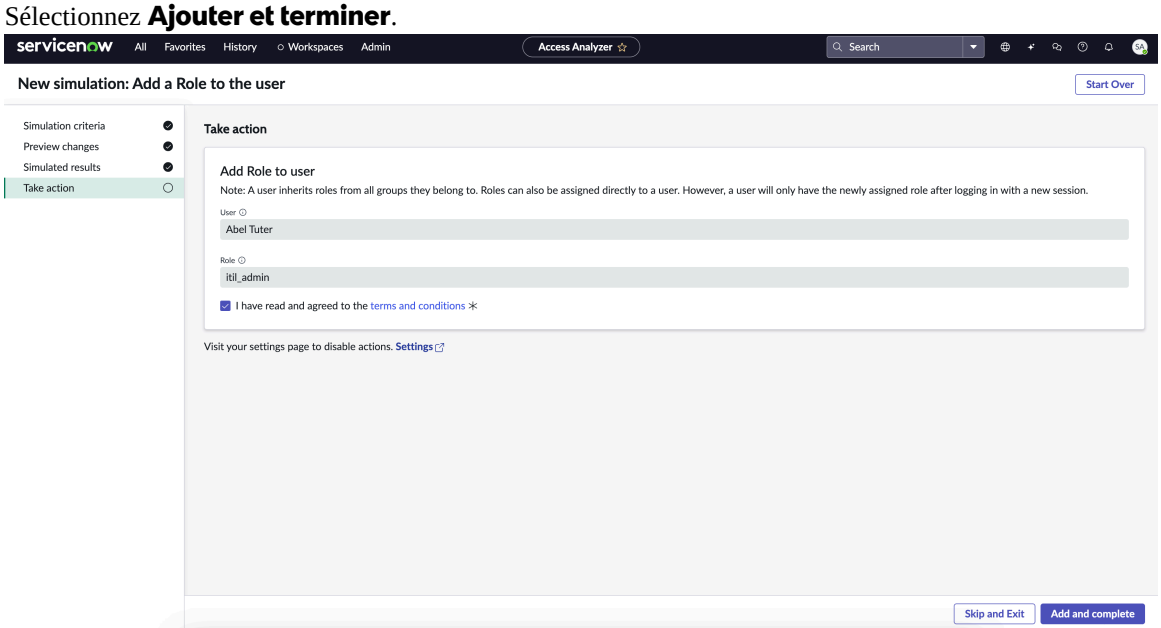


L'ajout du **itil_admin** permet à l'utilisateur d'effectuer une opération de suppression sur la table (incident).

Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez redémarrer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Ajouter et terminer**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer des actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

Les rôles sont ajoutés avec succès à l'utilisateur. Vous pouvez vérifier l'accès à l'aide de l'analyseur d'accès. Pour plus d'informations sur la vérification de l'accès d'un utilisateur, reportez-vous à la section Analyseur d'accès.

Suppression des rôles des utilisateurs

Utilisez le **rôle Simuler la suppression pour simuler** les changements d'accès de l'utilisateur pour une ressource (tables).

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Activez l'option Prendre des mesures. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Procédure

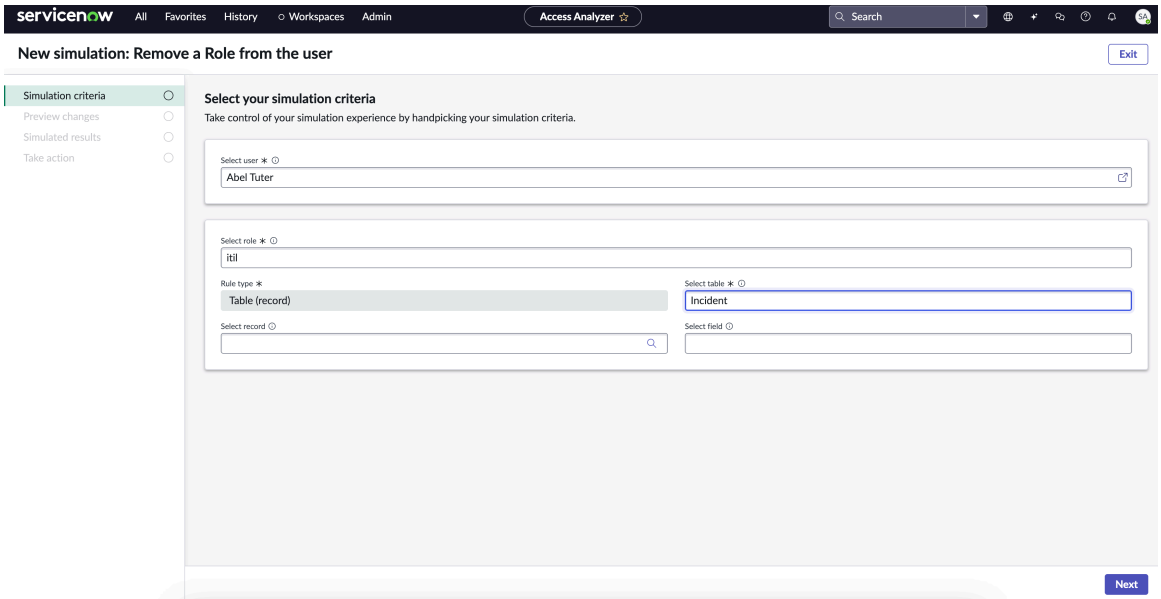
1. Accédez à la **Tous** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Supprimer un rôle de l'utilisateur.
3. Spécifiez les champs suivants pour vos critères de simulation :

Supprimer un rôle de l'utilisateur

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un rôle *	Spécifiez un rôle à sélectionner dans la liste. Dans cet exemple, **itil**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ peut être utilisé pour analyser l'autorisation même au niveau du champ. Par exemple, Actif, Créé par, etc.

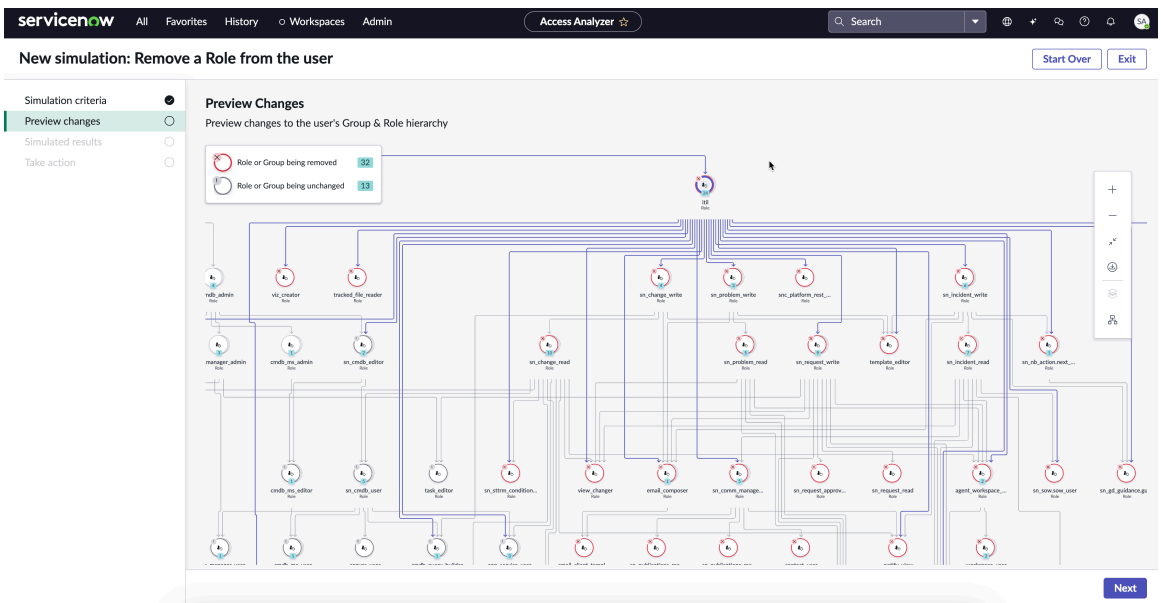
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez **Suivant**.

5. Prévisualisez les modifications.
   Les rôles supprimés sont simulés dans les modifications apportées à l'aperçu. Vous pouvez valider les rôles et les rôles enfants qui sont supprimés pour l'utilisateur avant de passer à l'étape suivante.

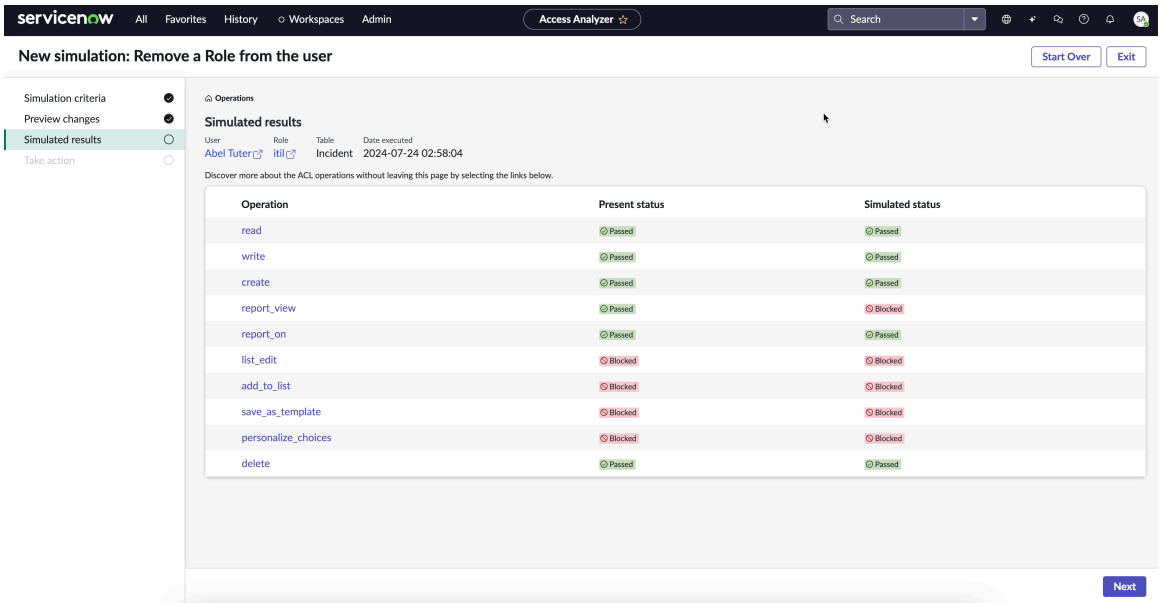


6. Sélectionnez **Suivant**.

7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez redémarrer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Supprimer et terminer**.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer des actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

Les rôles sont supprimés avec succès de l'utilisateur. Vous pouvez vérifier l'accès à l'aide de l'analyseur d'accès. Pour plus d'informations sur la vérification de l'accès d'un utilisateur, reportez-vous à la section Analyseur d'accès.

Ajout d'utilisateurs à des groupes

Utilisez **Simuler Ajouter au groupe** pour simuler les changements d'accès de l'utilisateur pour une ressource (tables) lorsque l'utilisateur est ajouté à un groupe.

Avant de commencer
Rôle requis : admin, access_analyzer_admin

Activez l'option Prendre des mesures. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Traduction automatique

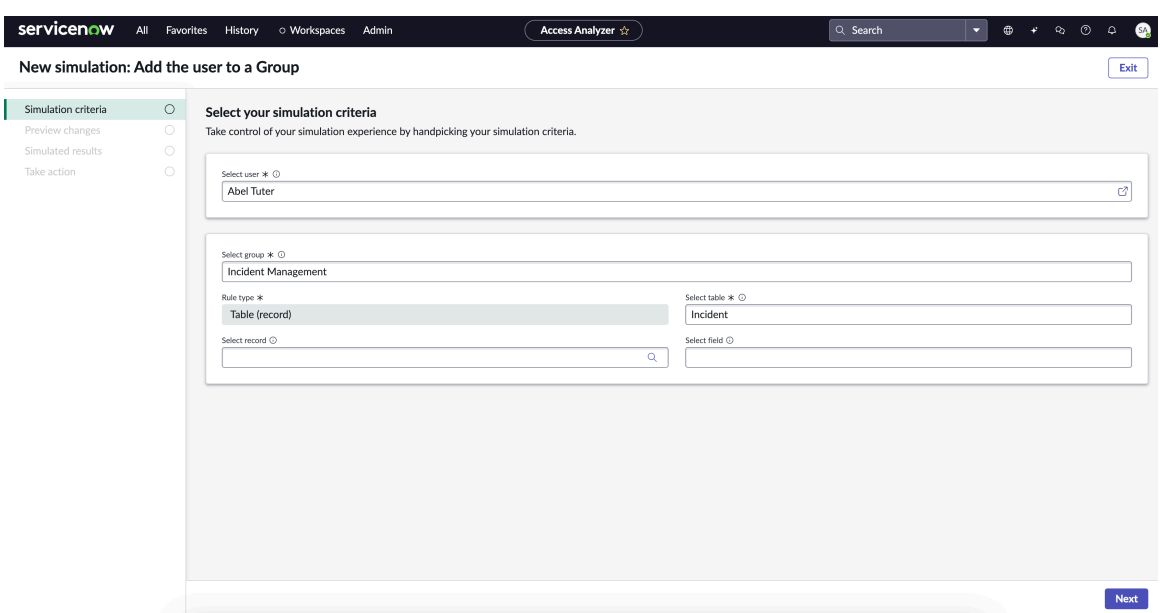
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Ajouter l'utilisateur à un groupe.
3. Spécifiez les champs suivants pour vos critères de simulation :

Ajouter l'utilisateur à un groupe

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un groupe *	Spécifiez un groupe à sélectionner dans la liste. Dans cet exemple, **Gestion des incidents**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ peut être utilisé pour analyser l'autorisation même au niveau du champ. Par exemple, Actif, Créé par, etc.

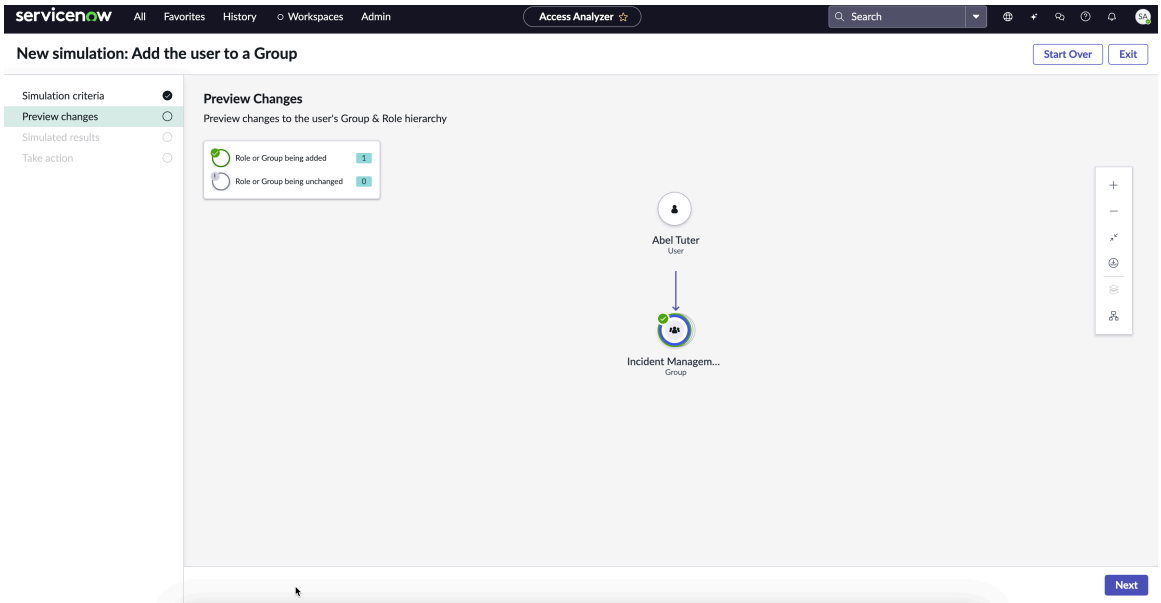


4. Sélectionnez **Suivant**.
5. Prévisualisez les modifications.

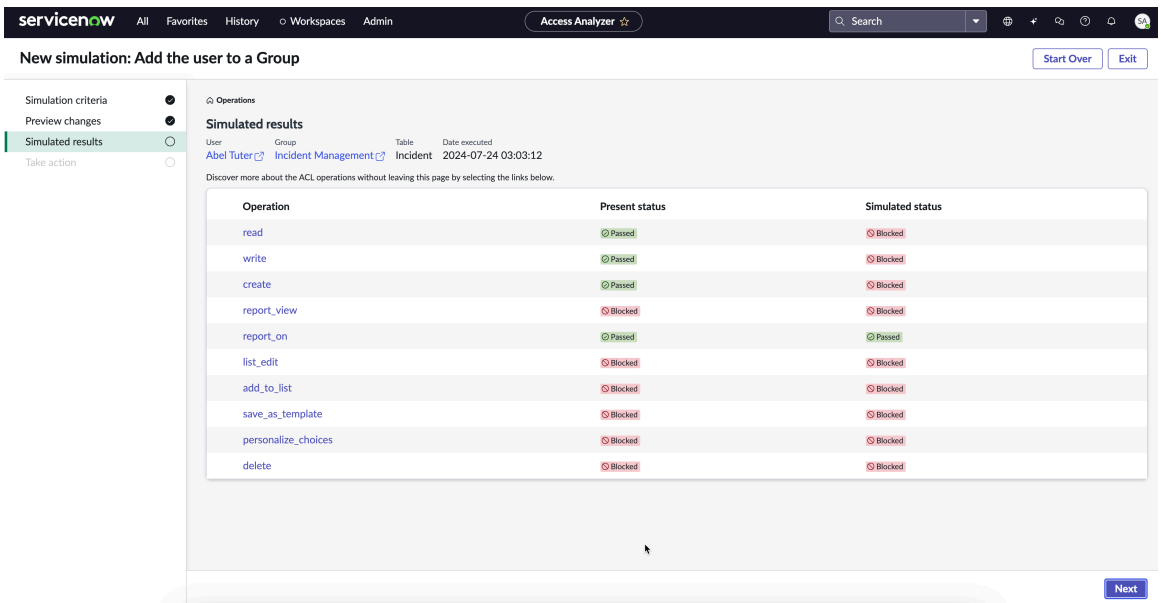
   Le groupe affecté à l'utilisateur est simulé dans les modifications apportées à l'aperçu. Vous pouvez valider les changements avant de passer à l'étape suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez redémarrer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Ajouter et terminer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer des actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

L'utilisateur est ajouté avec succès au groupe.

Suppression des utilisateurs des groupes

Utilisez **Simuler la suppression du groupe** pour simuler les changements d'accès de l'utilisateur à une ressource (tables) lorsque l'utilisateur est supprimé d'un groupe.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Activez l'option Prendre des mesures. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Procédure

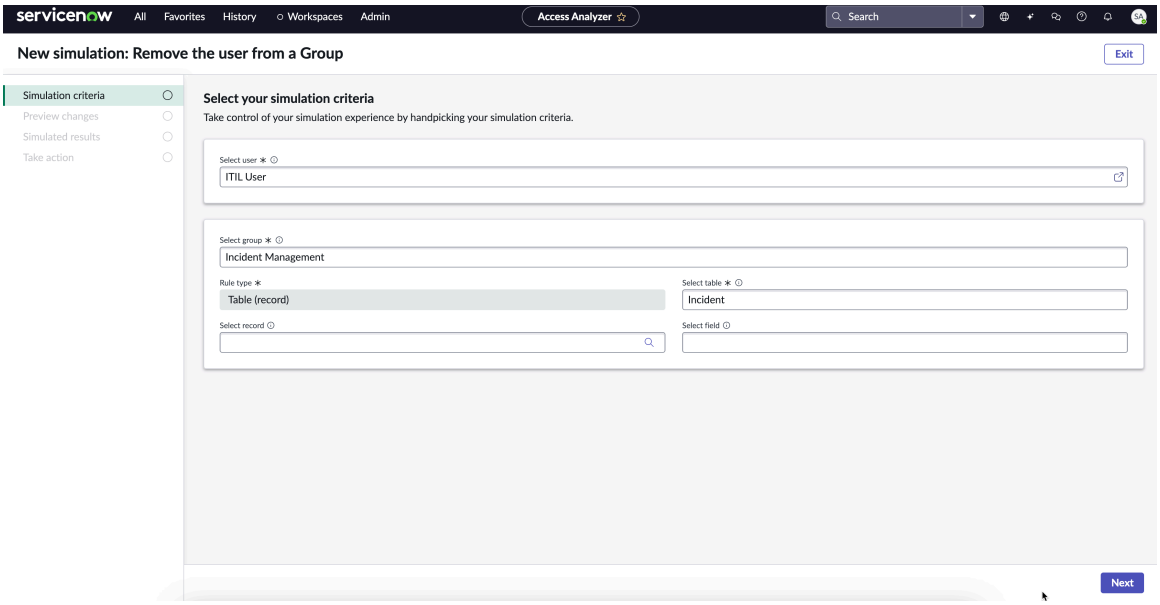
1. Accédez à la **Tous** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Retirer l'utilisateur d'un groupe.
3. Spécifiez les champs suivants pour vos critères de simulation :

Supprimer l'utilisateur d'un groupe

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Utilisateur ITIL**.
Sélectionner un groupe *	Spécifiez un groupe à sélectionner dans la liste. Dans cet exemple, **Gestion des incidents**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ peut être utilisé pour analyser l'autorisation même au niveau du champ. Par exemple, Actif, Créé par, etc.

Traduction automatique

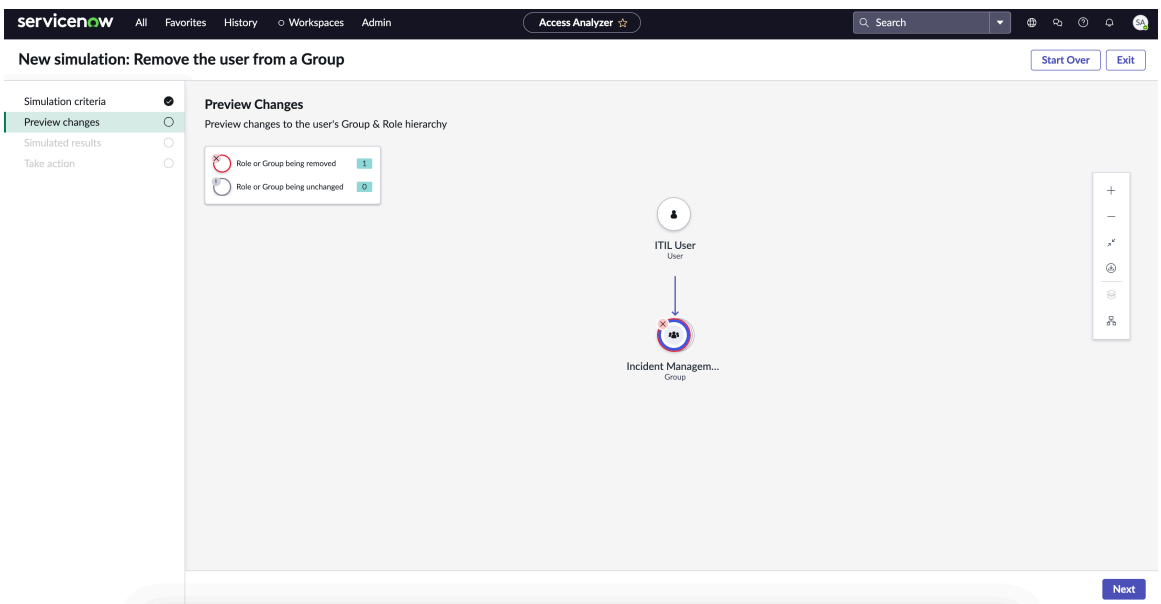
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d

4. Sélectionnez **Suivant**.
5. Prévisualisez les modifications.

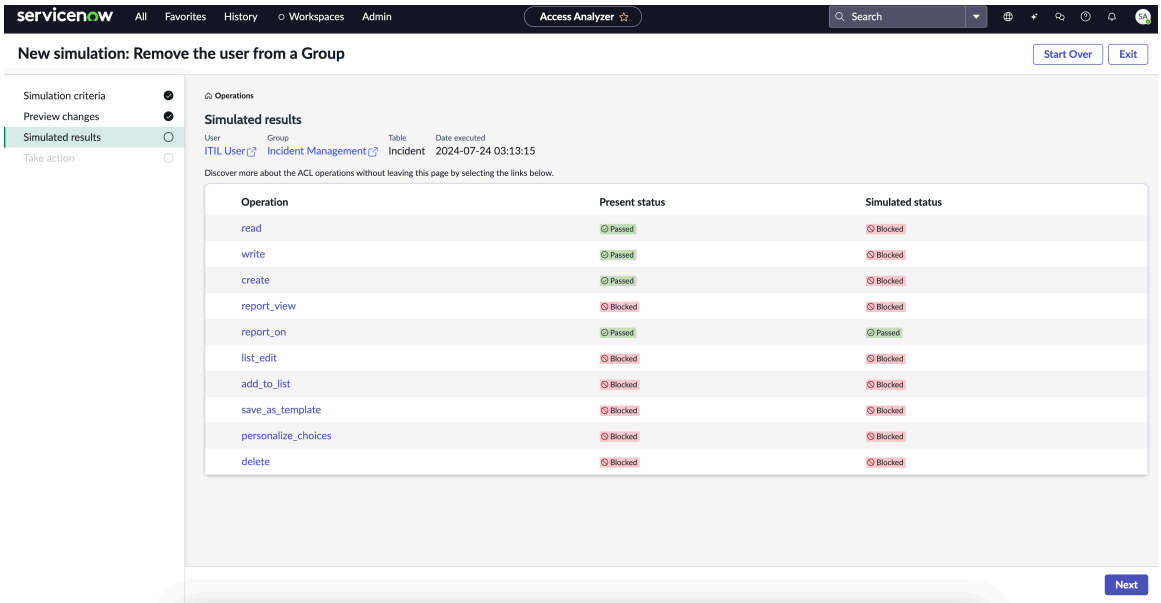
   Le groupe à partir duquel l'utilisateur est supprimé est simulé dans les modifications apportées à l'aperçu. Vous pouvez valider les changements avant de passer à l'étape suivante.



6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez redémarrer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Supprimer et terminer**.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer des actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

L'utilisateur est supprimé avec succès de l'utilisateur.

Forum aux questions

Questions fréquemment posées sur l'utilisation du simulateur d'accès.

Forum aux questions

Questions	Explication
Comment puis-je commencer à utiliser le simulateur ?	Vous pouvez sélectionner l'option Simuler pour les différents scénarios que vous souhaitez simuler pour les utilisateurs et suivre les étapes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum aux questions (suite)

Questions	Explication
Comment fonctionne le simulateur ?	Le simulateur d'accès simule l'accès à la table spécifiée pour l'utilisateur sélectionné et vous prévisualise les changements d'accès afin de prendre des décisions concernant la mise en service de l'accès.
Comment activer ou désactiver les actions dans le simulateur ?	Vous pouvez activer ou désactiver les actions dans le simulateur d'accès en accédant aux Paramètres ou pendant les étapes Prendre des mesures du processus de simulation.

Aperçus d'accès

Aperçus d’accès vous aide à gagner en confiance dans vos affectations de rôle ou de groupe.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Aperçus d’accès.

Configurer



Découvrez comment configurer Aperçus d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser



Sachez comment utiliser Aperçus d’accès.

Exploration d’Aperçus d’accès

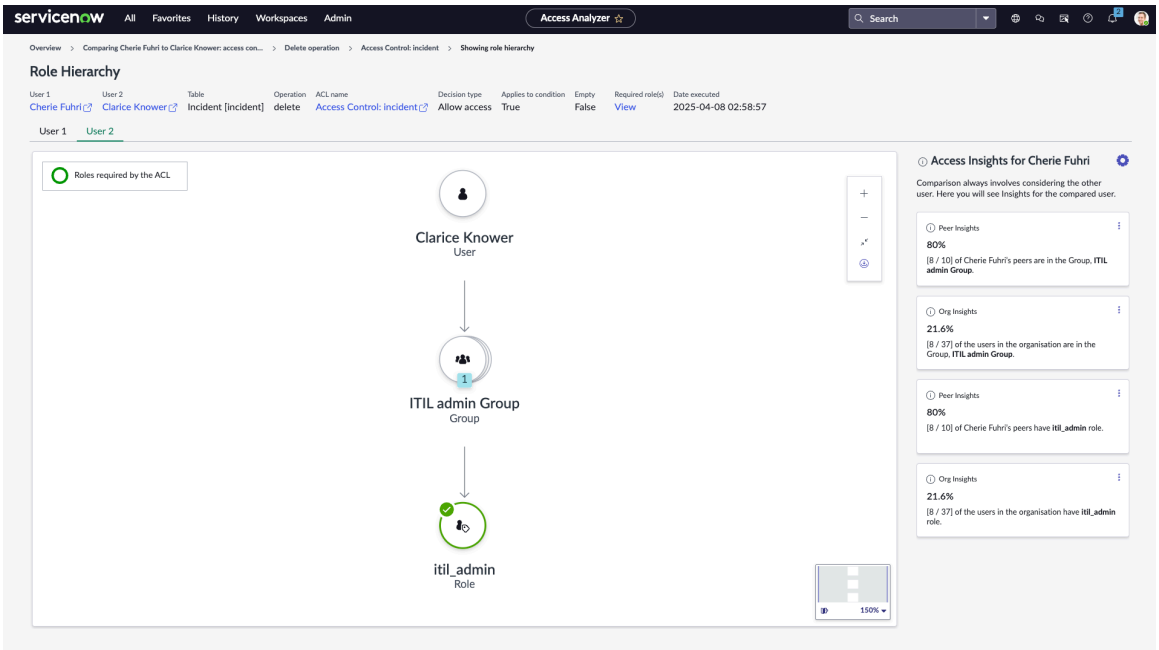
Les aperçus d’accès de l’analyseur d’accès vous aident à gagner en confiance dans vos affectations de rôle ou de groupe.

Aperçus d’accès affiche les statistiques de l’accès de votre utilisateur à une ressource au niveau des pairs et de l’organisation. Cela vous permet de voir si le rôle ou le groupe peut être affecté à l’utilisateur que vous examinez actuellement pour des autorisations supplémentaires. Cela vous aide à comparer les affectations de rôle et de groupe au sein du même groupe de pairs.

Les aperçus d’accès ne s’affichent que lors de la comparaison de l’accès de l’utilisateur à l’aide de la fonctionnalité Comparer l’accès de l’utilisateur de l’analyseur d’accès. Pour en savoir plus sur l’utilisation d’Aperçus d’accès, reportez-vous à la section Utilisation d’Aperçus d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En fonction des statistiques, vous pouvez décider de fournir les affectations de rôle ou de groupe correctes aux utilisateurs que vous comparez au sein de leurs pairs.

Remarque :

- Access Insights est disponible avec Access Analyzer V4.
- Vous devez comparer les utilisateurs au niveau des pairs (même organisation, même département, même gestionnaire) tout en visualisant les statistiques dans la fonctionnalité Aperçus d'accès.

Pour activer Aperçus d'accès dans l'analyseur d'accès, vous devez accéder aux paramètres. Pour en savoir plus, consultez Configuration d'Aperçus d'accès.

Configuration d'Aperçus d'accès

Activez la fonctionnalité Aperçus d'accès dans l'analyseur d'accès.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

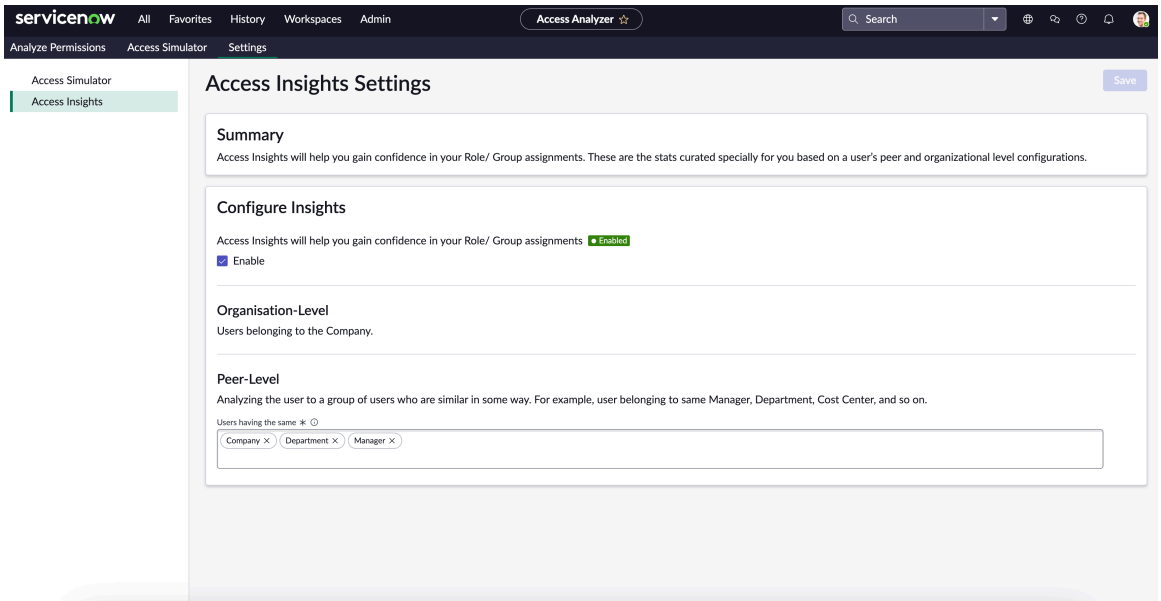
Dans la procédure suivante, nous vous expliquons les étapes d'activation d'Aperçus d'accès.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser l'accès**.
2. Sélectionnez l'onglet **Paramètres**.
3. Sélectionnez **Aperçus d'accès**.
4. Activez **Aperçus d'accès**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Par défaut, les champs Niveau des pairs sont sélectionnés avec **Société**, **Département**, **Gestionnaire**. Vous pouvez ajouter d'autres champs tels que **Centre de coûts**, **Code du pays**, **Emplacement** et **Titre**.

5. Sélectionnez **Enregistrer**.

Résultats

La fonctionnalité Aperçus d'accès est activée et affichée lorsque vous affichez la **hiérarchie des rôles** tout en comparant l'accès utilisateur à une ressource. Pour en savoir plus sur l'utilisation d'Aperçus d'accès, reportez-vous à la section Utilisation d'Aperçus d'accès.

Utilisation d'Aperçus d'accès

Utilisez Aperçus d'accès pour comprendre l'accès des utilisateurs au niveau des pairs à une ressource sélectionnée.

Avant de commencer

Rôle requis : admin, access_analyzer_admin

Remarque :
Pour afficher les détails de la fonctionnalité Aperçus d'accès, vous devez utiliser la fonctionnalité Comparer l'accès utilisateur .

Dans la procédure suivante, nous vous expliquons les étapes d'affichage des statistiques d'affectation de rôle ou de groupe au niveau des pairs dans la fonctionnalité Aperçus d'accès.

Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Comparer l'accès de l'utilisateur** .
3. Renseignez les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparer l'accès de l'utilisateur

Champ	Description
Sélectionner l’utilisateur 1*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour comparaison.
Sélectionner l’utilisateur 2*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour le comparer à l’utilisateur 1.
Type de règle*	Analysez les autorisations d’accès pour une table. **Remarque :** Seules les autorisations d’accès à une table peuvent être utilisées dans **l’accès utilisateur de comparaison**.
Sélectionner une table*	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d’enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

4. Sélectionnez **Comparer l’accès utilisateur**.

   Les résultats **de comparaison de l’accès utilisateur** pour les utilisateurs sélectionnés s’affichent.

   La comparaison des résultats de l’accès utilisateur affiche l’opération et l’état d’évaluation de l’accès pour les utilisateurs. Par exemple, Charlier Fuhri et Charlie Knower.

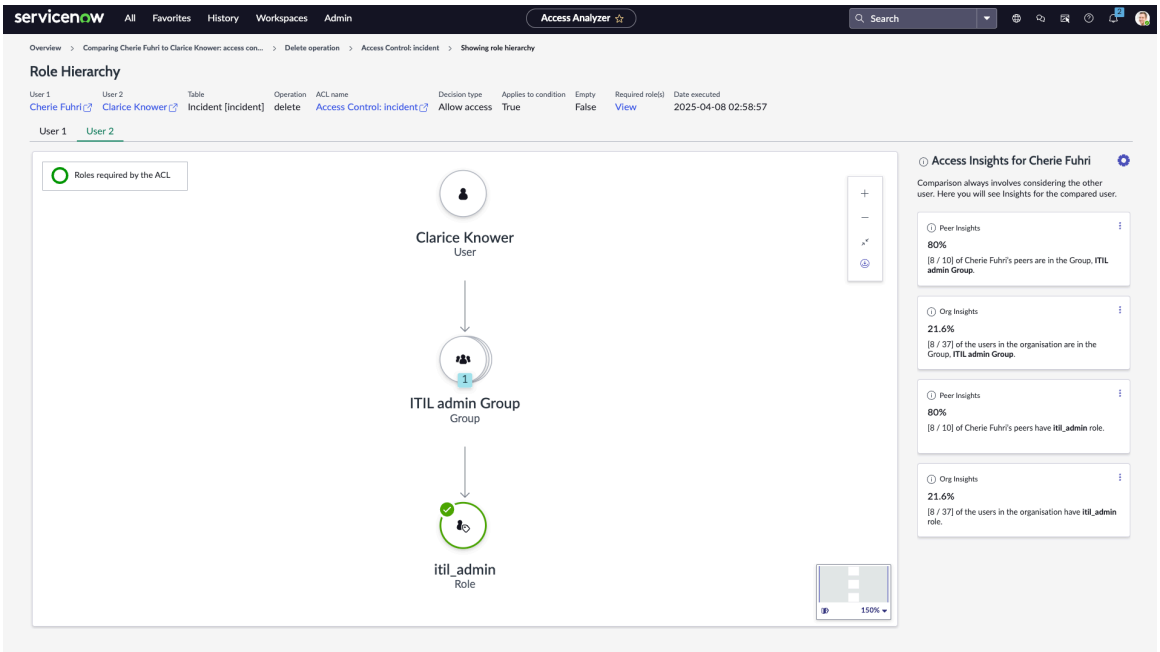
5. Sélectionnez une opération.
   Par exemple, **opération de lecture** .
6. Sélectionnez l’un des **contrôles d’accès** pour en savoir plus sur l’accès.
7. Sélectionnez **Afficher la hiérarchie des rôles** pour afficher la comparaison d’accès au niveau d’un accès au niveau des pairs.

   Les aperçus d’accès s’affichent comme suit :

   - **Aperçus des pairs** : affiche le nombre d’utilisateurs ayant le même rôle affecté au sein de leurs pairs (le même gestionnaire ou département).
   - **Aperçus de l’organisation** : affiche le nombre d’utilisateurs ayant le même rôle affecté au sein de l’organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En fonction de ces informations, vous pouvez choisir de fournir ou de révoquer l'accès à l'utilisateur que vous avez comparé.

Identité globale

Global Identity est un ServiceNow® produit qui permet d'identifier des utilisateurs uniques sur plusieurs instances.

Global Identity permet de gérer les utilisateurs, leurs attributs et d'autres données fondamentales sur ServiceNow® plusieurs ServiceNow® instances.

Explorer l'ID fédéré



Accéder à l'ID fédéré



Découvrez les principales fonctionnalités et la valeur commerciale de Federated ID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Accéder à l’ID fédéré.
Mise à jour des champs d’ID  Mettez à jour et configurez l’ID fédéré.	

Explorer l’ID fédéré

Déterminez les utilisateurs sur plusieurs instances en fonction du nom d’utilisateur et de l’adresse e-mail, et fournissez un ID unique (ID fédéré) à l’utilisateur de toutes les instances.

L’ID fédéré est utilisé pour identifier les utilisateurs dans plusieurs ServiceNow® instances. L’ID fédéré permet d’identifier l’utilisateur et de déterminer le nombre précis d’utilisateurs sur plusieurs instances. Pour plus d’informations, consultez ID fédéré.

Remarque :
Le nom d’utilisateur est requis pour générer des ID fédérés.

L’ID fédéré est un identificateur unique d’identité utilisant une fonction de hachage entre les ServiceNow® instances.

En utilisant **l’ID d’utilisateur** et **l’adresse e-mail** de l’utilisateur dans toutes les instances, l’ID fédéré est créé et affiché dans la table sys_user.

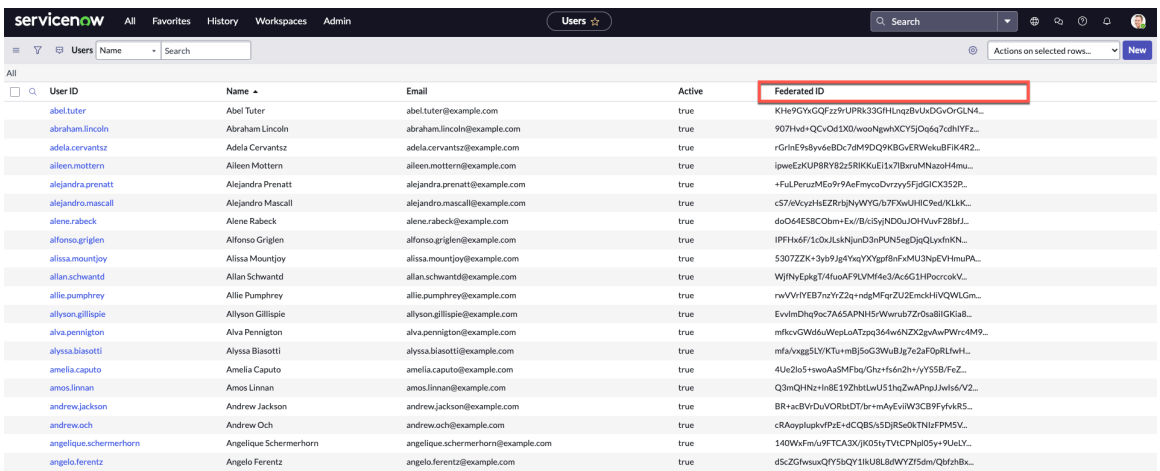
Après la mise à niveau vers la Yokohama version, le module d’extension Federated ID Generation (com.glide.identity.globalid) est automatiquement installé sur toutes les instances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'e-mail sont utilisés par défaut pour générer des ID fédérés. Pour mettre à jour les champs permettant de générer des ID fédérés en fonction de vos besoins, reportez-vous à la section Mise à jour des champs d'ID.
- **Iamsync_admin** rôle est requis pour mettre à jour la configuration.
- S'il existe des utilisateurs avec des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré n'est généré que pour un seul utilisateur. Si le nom d'utilisateur est nul ou vide, l'ID fédéré est nul.



Les changements de schéma après l'installation du module d'extension sont les suivants :

- Une nouvelle federated_id de colonne dans la table sys_user est créée.
- Nouvelle table iamsync_type est automatiquement remplie avec la configuration par défaut de la table sys_user .

L'ID fédéré n'est pris en charge que pour la table sys_user et toutes les tables qui étendent la table sys_user.

Après la mise à niveau vers la Yokohama version, le module d'extension Federated ID Generation (com.glide.identity.globalid) est automatiquement installé sur toutes les instances.

Accès aux critères d'ID fédéré

Critères d'accès à l'ID fédéré pour connaître les champs d'ID utilisés pour générer l'ID fédéré.

Avant de commencer

Rôle requis : iamsync_admin

Procédure

1. Accédez à la **Tous** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. La page Critères d'ID fédéré affiche l'enregistrement avec les détails suivants :

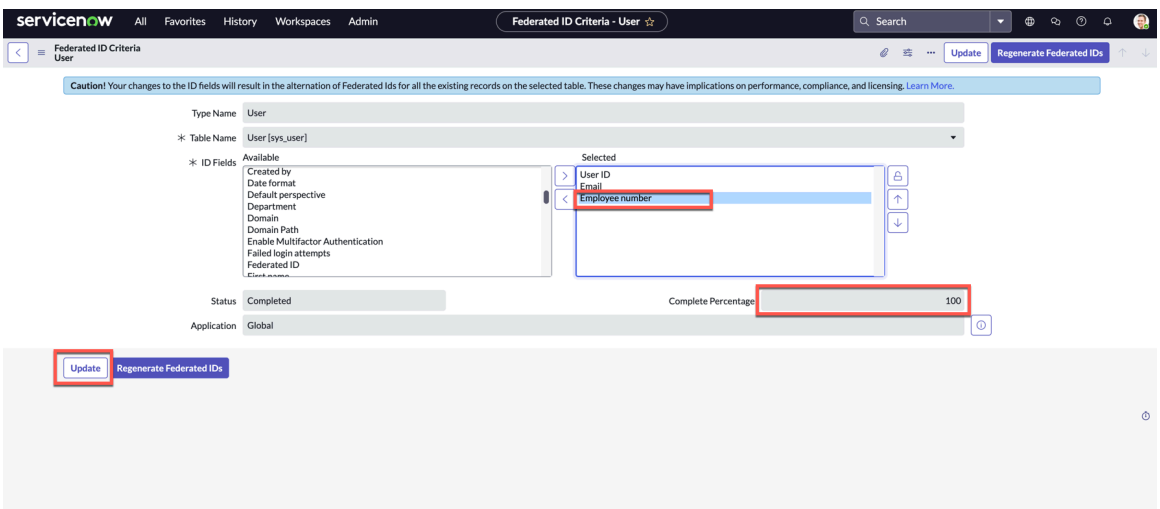
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Nom du type : **Utilisateur**
- Nom de la table : **Utilisateur [sys_user]**
- Champs d'ID : **user_name (ID d'utilisateur), e-mail** (champs par défaut utilisés pour la génération d'ID fédérés).
- État : **terminé** (état de génération d'ID fédérés). État disponible : **Prêt**, **En cours d'exécution**, **Terminé**, **Erreur**.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'e-mail sont utilisés par défaut pour générer des ID fédérés.



Remarque :
Seuls les champs d'ID peuvent être mis à jour pour générer un nouvel ID fédéré pour les enregistrements existants. Pour en savoir plus, reportez-vous à la section Mise à jour des champs d'ID.

Mise à jour des champs d'ID

Mettez à jour les champs d'ID pour régénérer les ID fédérés en fonction des champs mis à jour.

Avant de commencer

Rôle requis : iamsync_admin

Remarque :
Tout changement apporté aux champs d'ID entraîne le changement des ID fédérés pour tous les enregistrements existants sur la table sélectionnée. Ces changements peuvent avoir des répercussions sur les performances, la conformité et la gestion des licences.

Procédure

1. Accédez à la **Tous** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. Sélectionnez le nom du type (**Utilisateur**).
3. Sélectionnez les nouveaux champs d'ID de la page Critères d'ID fédérés que vous souhaitez ajouter à partir de Disponible pour la sélection à l'aide des flèches de direction.

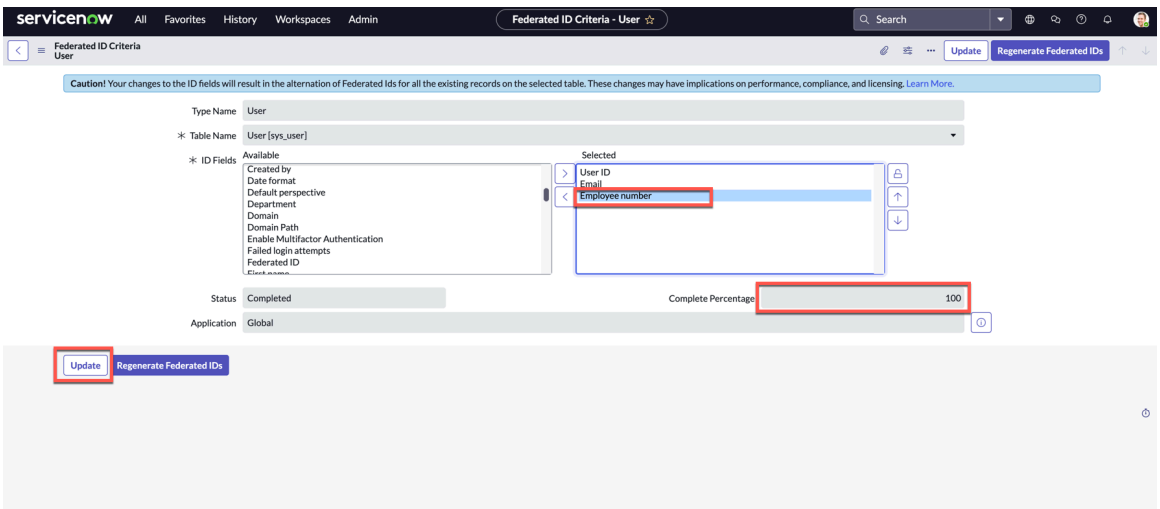
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, **le numéro d'employé**.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'e-mail sont utilisés par défaut pour générer des ID fédérés.
- S'il existe des utilisateurs avec des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré n'est généré que pour un seul utilisateur. Si le nom d'utilisateur est nul ou vide, l'ID fédéré est nul.



Maintenant, le **numéro d'employé** sélectionné devient un autre attribut pour générer l'ID fédéré.

4. Sélectionnez **Mettre à jour** pour générer des ID fédérés.

Remarque :
Sélectionnez d'abord **Mettre à jour** , puis vérifiez le pourcentage d'achèvement (100) avant de lancer une autre mise à jour.

Le pourcentage d'état indique la génération d'ID fédérés pour toutes les identités entre les instances.

Remarque :

- Tant que la tâche de mise à jour précédente n'est pas terminée, ne modifiez pas le champ.
- Les champs mis à jour doivent être de type chaîne.
- Les champs qui ne peuvent pas être sélectionnés en tant que champs d'ID sont les suivants :
  - Champs au niveau du système
  - Champs de chiffrement Edge
  - Champs de mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Accédez à la table sys_user pour afficher les nouveaux ID fédérés générés suite à la mise à jour des champs d'ID.

Remarque :
Sélectionnez **Régénérer les ID fédérés** si un utilisateur est créé ou mis à jour via des importations XML, des mises à jour de base de données de bas niveau, si l'instance ne fonctionne pas correctement. **Sélectionner Régénérer les ID fédérés** régénère les ID de tous les utilisateurs, à l'aide des critères du champ d'ID actuel.

Audit d'identité et d'accès

Utilisez l'audit d'identité et d'accès pour comprendre les changements apportés aux utilisateurs, aux groupes, aux rôles et aux ACL.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l'audit d'identité et d'accès.

Configurer



Découvrez comment configurer l'audit d'identité et d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats d'audit



Affichez les résultats de l'audit d'identité et d'accès.

Exploration de l'audit d'identité et d'accès

Utilisez l'audit d'identité et d'accès pour comprendre les changements apportés aux utilisateurs, aux groupes, aux rôles et aux ACL.

L'audit d'identité et d'accès permet de comprendre les informations essentielles sur qui a modifié quoi, où et quand dans les comptes, groupes et rôles d'utilisateurs.

Permet de détecter les utilisateurs malveillants, de suivre les activités inhabituelles dans l'instance et de respecter les ServiceNow® normes de conformité en matière de suivi des changements d'accès.

Identity and Access Audit (Identity Security Audit) est un module d'extension (`com.glide.security.audit`) qui est installé automatiquement.

La fonctionnalité d'audit peut être activée ou désactivée en activant la propriété système`glide.identity.security.audit.enabled` . Par défaut, cette propriété est définie sur `true`.

L'audit d'identité et d'accès vous permet d'effectuer les actions suivantes :

- Affichez les modifications apportées au cours des 30 derniers jours aux utilisateurs, aux groupes, aux attributs d'ACL de rôle, aux appartenances aux rôles, aux adhésions à des groupes et aux rôles ACL.
- Suivez les changements dans votre ServiceNow instance.
- Aidez à atténuer les risques potentiels en matière de sécurité et de réglementation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Démontrez la conformité auprès des auditeurs des différents groupes au sein de l'organisation.
- Démontrez que l'organisation n'est pas vulnérable aux menaces liées au manque de visibilité du groupe d'utilisateurs et aux changements de rôles.

Profils d'utilisateurs dans Identity Access and Audit

Les différents profils d'utilisateur dans l'audit d'identité et d'accès sont les suivants :

- **Administrateur** : affichez les enregistrements d'audit et la configuration.
- **Administrateur de sécurité** : affichez ces pistes d'audit. Modifiez la configuration pour activer ou désactiver l'audit pour une certaine table ou modifier les champs en cours d'audit.

Tables d'audit

Les tables suivantes peuvent être auditées à l'aide de l'audit d'identité et d'accès :

- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d'accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d'utilisateur [sys_user_has_role]
- Rôles d'accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Modules de l'audit d'identité et d'accès

L'audit d'identité et d'accès possède les modules suivants sur l'instance ServiceNow :

Module	Description
Résultats d'audit	Affiche les audits qui se sont produits dans l'instance ServiceNow .
Configurer la table et les champs	Configurez les tables et les champs système avec les champs disponibles à partir de l'audit d'identité et d'accès.
Configurer la période de conservation	Configurez la période de conservation des données auditées. La période maximale pouvant être définie est de 30 jours.
Pistes d'utilisateurs	Affiche les audits des utilisateurs.
Pistes de groupes	Affiche les audits des groupes.
Pistes des rôles	Affiche les audits des rôles.
Pistes ACL	Affiche les audits des ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats d'audit d'identité

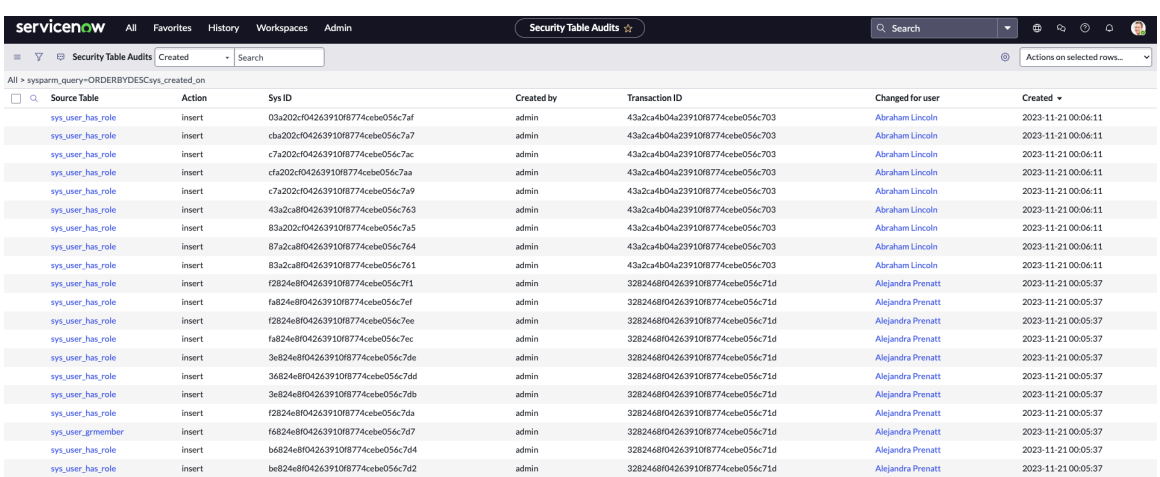
Affiche les audits qui se sont produits dans l'instance ServiceNow® .

Les résultats de l'audit affichent les changements apportés pour les utilisateurs, les groupes, les rôles et les ACL dans l'instance ServiceNow .

Pour accéder aux résultats de l'audit, naviguez **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Résultats d'audit**. La page Audits de tables de sécurité s'affiche avec les informations suivantes.

Audits de tables de sécurité

Nom de colonne	Description
Table source	Détails de la table source où l'audit a eu lieu.
Action	Décrit l'action de l'audit.
Sys_id	Détails sur le sys_id de l'enregistrement audité.
Créé par	Détails de l'audit qui a été créé par.
ID de transaction	ID unique qui représente chaque action sur l'audit particulier effectué.
Utilisateur concerné par le changement	Nom de l'utilisateur au moment de l'audit.
Créées	Heure et date d'exécution de l'audit.



Pistes d'utilisateurs

Affiche les audits des utilisateurs de l'instance ServiceNow® .

Les pistes d'utilisateurs affichent les changements d'attributs d'identité, les changements d'appartenance à un rôle et les changements d'appartenance à un groupe pour un utilisateur.

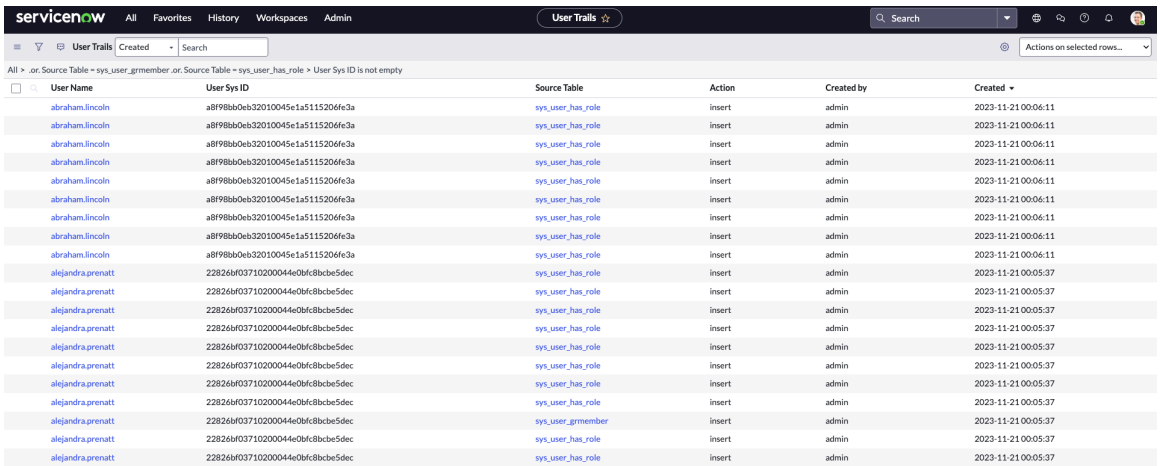
Pour accéder aux pistes d'utilisateurs, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes d'utilisateurs**. La page Pistes d'utilisateurs s'affiche avec les informations suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pistes d'utilisateurs

Nom d'utilisateur	Nom de l'utilisateur.
ID système de l’utilisateur	Détails sur l’utilisateur sys_id pour l’enregistrement audité.
Table source	Détails sur la table source où l’audit a été effectué.
Action	Décrit l’action de l’audit.
Créés par	L’utilisateur qui a effectué le changement.
Créées	Heure et date d’exécution de l’audit.



Pistes de groupes

Affiche les audits des groupes de l’instance ServiceNow® .

Les pistes de groupe affichent les changements d’attribut, d’appartenance et de rôle d’un groupe.

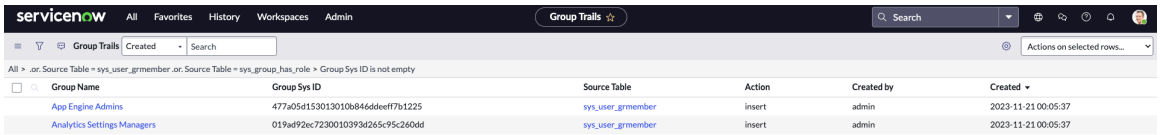
Pour accéder aux pistes de groupe, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes de groupes**. La page Pistes de groupe s’affiche avec les informations suivantes.

Pistes de groupes

Nom de groupe	Nom du groupe.
ID système du groupe	Détails sur le groupe sys_id pour l’enregistrement audité.
Table source	Détails sur la table source dans laquelle l’audit a été effectué.
Action	Décrit l’action de l’audit.
Créés par	L’utilisateur qui a effectué le changement.
Créées	Heure et date d’exécution de l’audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pistes des rôles

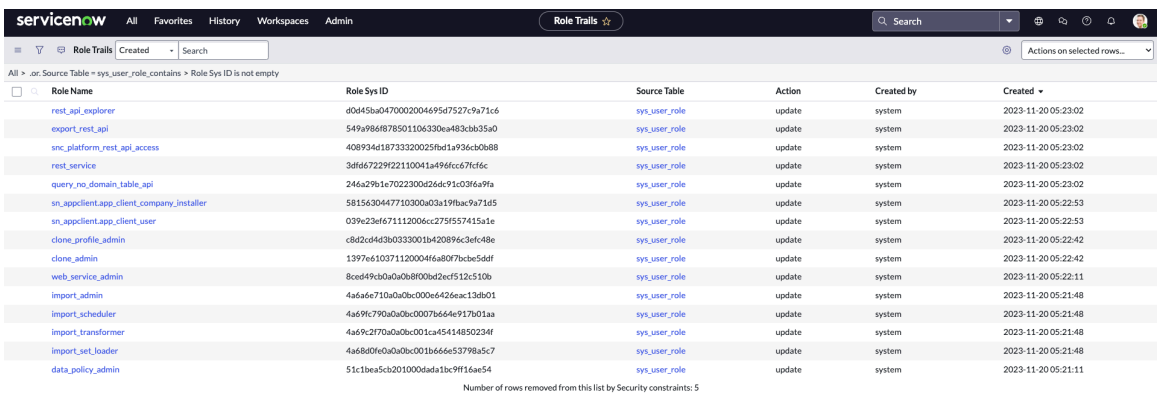
Affiche les audits des rôles de l'instance ServiceNow® .

Les pistes de rôle affichent les changements d'attributs et les changements de relation parent-enfant pour un rôle.

Pour accéder aux pistes de rôles, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes des rôles**. La page Pistes des rôles s'affiche avec les informations suivantes.

Pistes des rôles

Nom de rôle	Nom du rôle.
ID système du rôle	Détails sur le rôle sys_id pour l'enregistrement audité.
Table source	Détails sur la table source dans laquelle l'audit a été effectué.
Action	Décrit l'action de l'audit.
Créés par	L'utilisateur qui a effectué le changement.
Créées	Heure et date d'exécution de l'audit.



Pistes ACL

Affiche les audits des ACL de l'instance ServiceNow® .

Traduction automatique

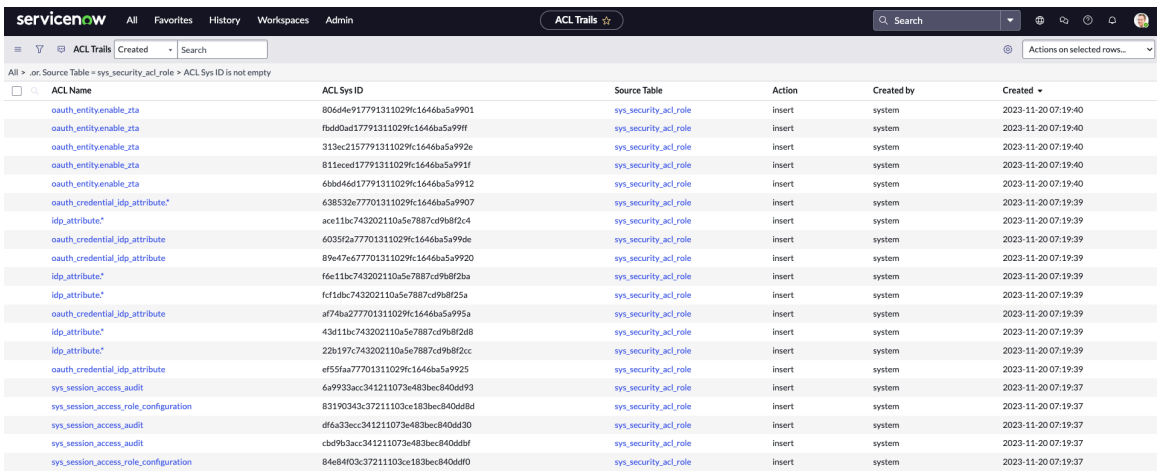
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les pistes d'ACL affichent les changements d'attributs et les changements de relation de rôle requis pour un ACL.

Pour accéder aux pistes ACL, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes ACL**. La page Pistes ACL s'affiche avec les informations suivantes.

Pistes ACL

Nom ACL	Nom de l'ACL.
ID système ACL	Détails sur l'ACL sys_id pour l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action de l'audit.
Créés par	L'utilisateur qui a effectué le changement.
Créées	Heure et date d'exécution de l'audit.



Champs auditables de sécurité

Affiche les détails au niveau de la table et du champ qui seront audités dans l'instance ServiceNow® .

La section Champs auditables de sécurité affiche les détails des tables et des champs qui seront audités dans l'instance ServiceNow .

Pour accéder à la page Champs auditables de sécurité, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer les tables et les champs**. La page Champs auditables de sécurité s'affiche avec les informations suivantes.

Champs auditables de sécurité

Nom de colonne	Description
Table à Audit	Détails de la table qui est auditée.
Destination de stockage d'audit	Détails de la destination où les détails de l'audit sont stockés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs auditables de sécurité (suite)

Nom de colonne	Description
Liste des champs	L'audit sera effectué pour les champs spécifiés dans la liste.
Créer	Auditez les changements associés à l'opération de création.
Mettre à jour	Vérifiez les changements associés à l'opération de mise à jour.
Supprimer	Vérifiez les changements associés à l'opération de suppression.
Actif	Auditez uniquement si la configuration de la table est active.



Les tables suivantes peuvent être auditées à l'aide de l'audit d'identité et d'accès :

- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d'accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d'utilisateur [sys_user_has_role]
- Rôles d'accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Configuration des tables et des champs

Audit d'identité et d'accès pour comprendre les changements apportés à un utilisateur, un groupe, un rôle et un ACL.

Avant de commencer
Rôle requis : security_admin

Vous devez élever votre rôle à celui d'administrateur de sécurité pour configurer les tables et les champs pour l'audit d'identité et d'accès.

Les tables suivantes peuvent être configurées pour l'audit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

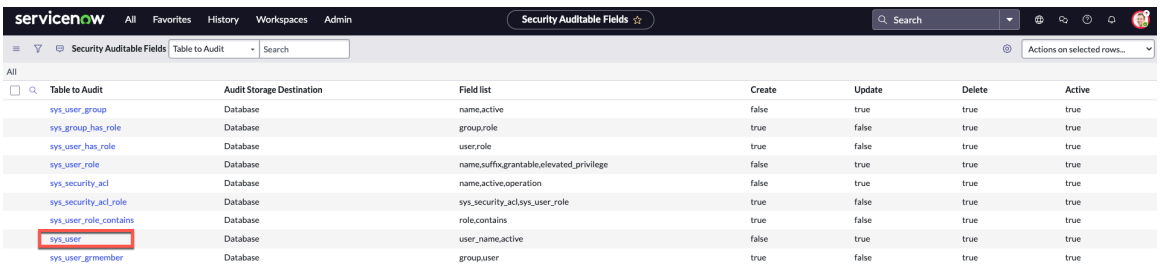
- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d’accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d’utilisateur [sys_user_has_role]
- Rôles d’accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Remarque :
Pour savoir quels champs peuvent être configurés pour les tables, reportez-vous à la section Champs pris en charge et non pris en charge dans Identity Access and Audit.

Procédure

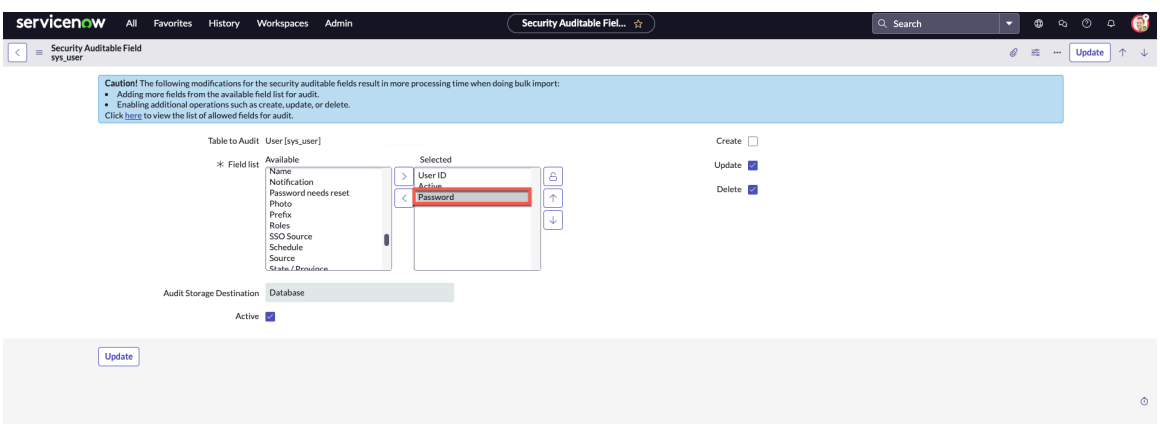
1. Accédez à la **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer les tables et les champs**.
2. Sélectionnez la table à partir de laquelle vous souhaitez auditer un champ.

   Par exemple, **sys_user**.



3. Ajoutez le champ à auditer.

   Par exemple, **Mot de passe**.



Traduction automatique

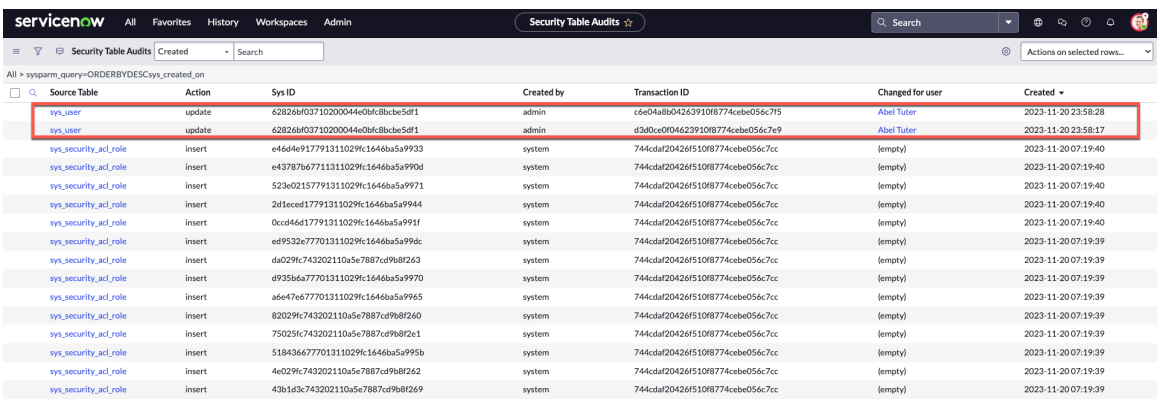
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les modifications suivantes apportées aux champs auditables de sécurité entraînent une augmentation du temps de traitement lors de l'importation en bloc :

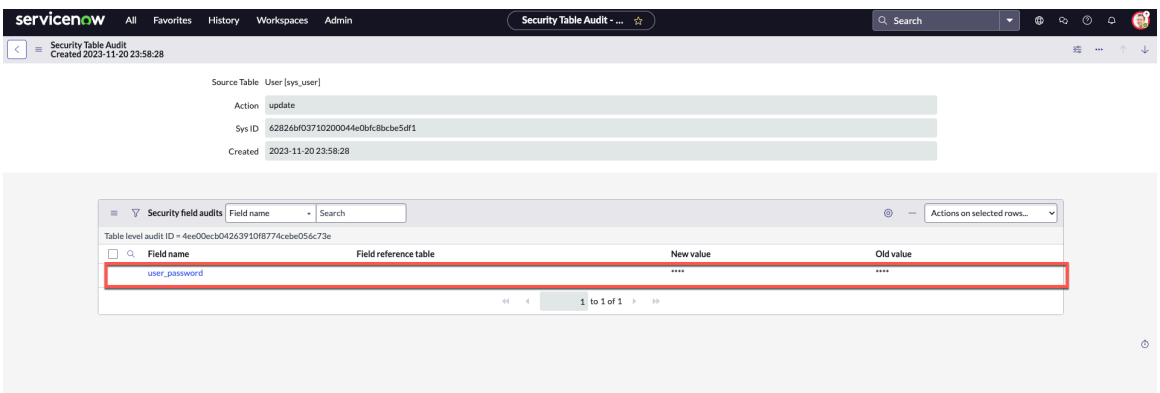
- Ajouter d'autres champs à partir de la liste de champs disponibles pour l'audit.
- Activation d'opérations supplémentaires telles que créer, mettre à jour ou supprimer.

4. Mettez à jour l'enregistrement

Tout changement apporté au champ du mot de passe ajoute un nouvel enregistrement aux audits de la table de sécurité. Dans cet exemple, l'audit affiche un champ Mot de passe modifié pour l'utilisateur **Abel Tuter**.



Sélectionnez l'enregistrement créé pour afficher les détails des changements.



Configuration de la période de conservation

Configurez la période de conservation pour l'audit d'identité et d'accès.

Avant de commencer

Rôle requis : admin

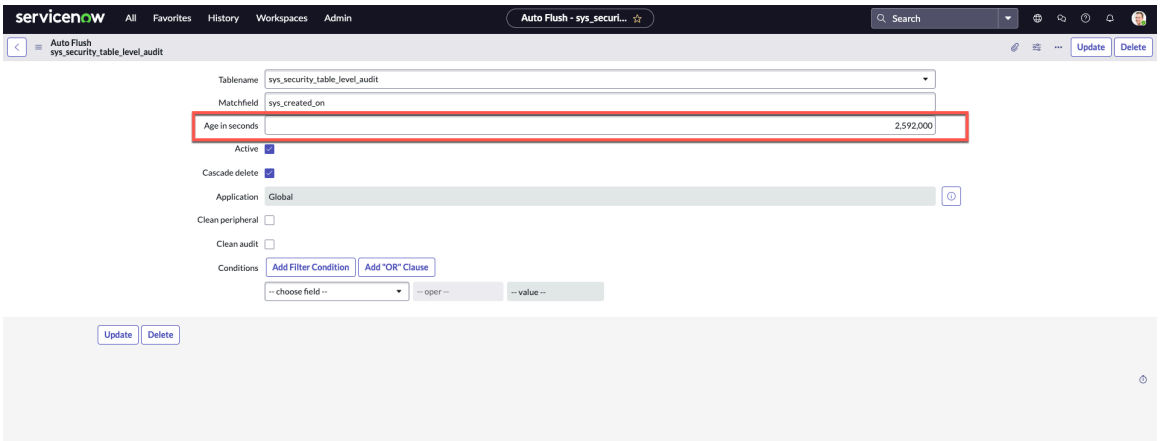
Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer la période de conservation**.
2. Sur le formulaire, vous pouvez modifier l'âge en secondes.

Remarque :
Le nombre maximal de jours pour l'audit d'identité et d'accès est de 30 jours (2 592 000 secondes).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur Enregistrer ou Mettre à jour pour enregistrer ou mettre à jour l'enregistrement.

Champs pris en charge et non pris en charge dans Identity Access and Audit

Liste des champs pris en charge et non pris en charge pour l'audit.

La validation des champs d'audit empêche de choisir certains champs dans le field_list de la table Configuration de l'audit de champ de sécurité (sys_sec_field_audit_config).

Champ pris en charge ou non pris en charge pour l'audit

Table	Champs pris en charge ou non pris en charge
Toutes les tables	Champs qui ne sont pas pris en charge : • Créé le (sys_created_on) • Créé par (sys_created_by) • Mis à jour par (sys_updated_by) • Date de mise à jour (sys_updated_on)
L'utilisateur a un rôle (sys_user_has_role)	Champs pris en charge : • Utilisateur • Rôle • Hérité • Nombre
Utilisateur (sys_user)	Champs qui ne sont pas pris en charge : • Dernière connexion (last_login) • Heure de la dernière connexion (last_login_time) • Dernière connexion à l'équipement (last_login_device)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ pris en charge ou non pris en charge pour l'audit (suite)

Table	Champs pris en charge ou non pris en charge
	• Activer l'authentification multifacteur (enable_multifactor_authn) • Perspective par défaut (default_perspective) • Intégration du calendrier (calendar_integration) • ID fédéré (federated_id) • Mot de passe à réinitialiser (password_needs_reset) • Tentatives infructueuses (failed_attempts) • Dernier mot de passe (last_password) • Serveur LDAP (ldap_server) • Verrouillé (locked_out) • Notification (notification) • Rôles (roles) • Domaine (sys_domain) • Chemin de domaine (sys_domain_path) • Format d'heure (time_format) • ID d'utilisateur haché (hashed_user_id) • Nom de classe (sys_class_name) • Nombre de modifications (sys_mod_count)

Identity Center

Vous permet de surveiller, gérer et minimiser les risques basés sur l'identité et les failles de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Identity Center.

Activer



Découvrez comment activer Identity Center.

Mesures d’identité pour les administrateurs



Sachez comment les autorisations sont évaluées.

Identity Center pour les utilisateurs



Obtenez des détails sur les questions fréquemment posées sur l’analyseur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer Identity Center

Identity Center est un ensemble d'attributs d'utilisateur, d'accès, d'appareils, d'historique de connexion, d'activité de sécurité et bien plus encore.

Identity Center offre des options pour surveiller, gérer et minimiser les risques basés sur l'identité et les failles de sécurité.

Identity Center est un guichet unique pour surveiller, gérer et minimiser les risques basés sur l'identité et les failles de sécurité sur ServiceNow.

Pour activer Identity Center, installez le module d'extension Identity Center (com.snc.identity_center). Identity Center est disponible pour l'utilisateur final qui peut afficher les détails des sessions actives, l'historique de connexion et les appareils de confiance avec Identity Center. Pour plus d'informations, reportez-vous à la section Identity Center pour les utilisateurs.

Activation d'Identity Center

Pour Identity Center, installez le module d'extension Identity Center (com.snc.identity_center).

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension Identity Center (com.snc.identity_center) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application.

Identity Center pour les utilisateurs

Affichez les détails de vos sessions actives, de votre historique de connexion et de vos appareils de confiance avec Identity Center.

Identity Center est une collection d'attributs d'utilisateur, d'appareils, d'historique de connexion, d'activités de sécurité et bien plus encore. Il fournit une vue à volet unique de toutes les données, avec des contrôles de sécurité supplémentaires et des options de notification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avec Identity Center, vous pouvez afficher les détails de vos sessions actives, de votre historique de connexion et de vos appareils de confiance.

Pour accéder à l'Identity Center pour les utilisateurs, accédez à l'une des options suivantes :

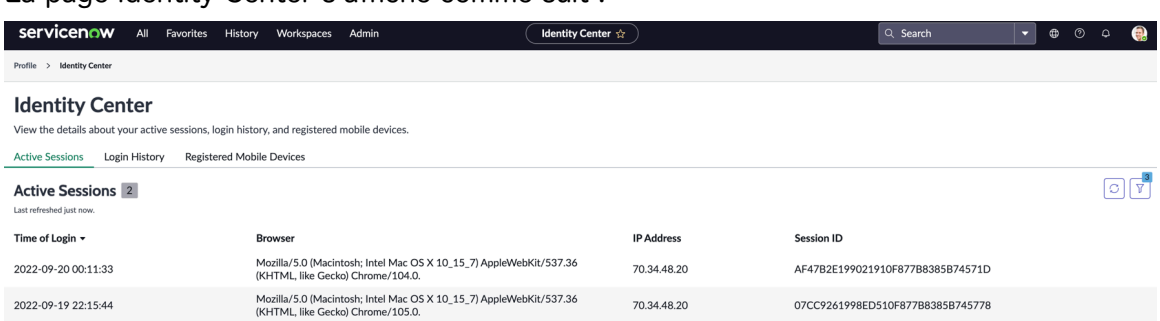
- Sur ServiceNow AI Platform, accédez à **Tous** > **Libre-service** > **Mon profil** et sélectionnez **Afficher Identity Center** dans la section Liens connexes.

  Remarque :
  Vous pouvez également accéder à votre profil en sélectionnant votre nom d'utilisateur dans l'en-tête de l'instance.



- Sur Now Support, sélectionnez le profil, puis sélectionnez **Afficher Identity Center** en bas de la page.

La page Identity Center s'affiche comme suit :



Identity Center comporte les onglets suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sessions actives
- Historique de connexion
- Équipements mobiles enregistrés

Vous pouvez sélectionner ces onglets pour afficher les détails tels que le navigateur, les adresses IP, les informations de relation de session, les informations de connexion, vos appareils mobiles enregistrés.

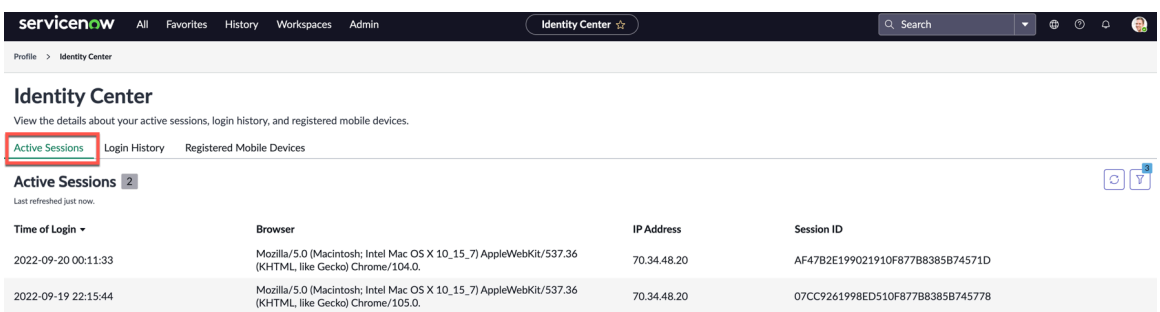
Affichage des sessions actives dans Identity Center

Affiche les informations sur les sessions utilisateur.

Les sessions actives sont les sessions ouvertes sur l'instance actuelle ServiceNow® avec différents navigateurs ou appareils.

L'onglet Sessions actives d'Identity Center vous aide à identifier vos sessions en fonction du navigateur, de l'adresse IP et de l'ID de sessions. À l'aide de ces informations, vous pouvez effectuer les actions requises, comme prolonger ou mettre fin à la session.

L'utilisation de ces informations peut aider à déterminer si les sessions sont réelles et ne constituent pas un problème de sécurité.



Affichage de l'historique de connexion dans Identity Center

Fournit des détails sur votre historique de connexion.

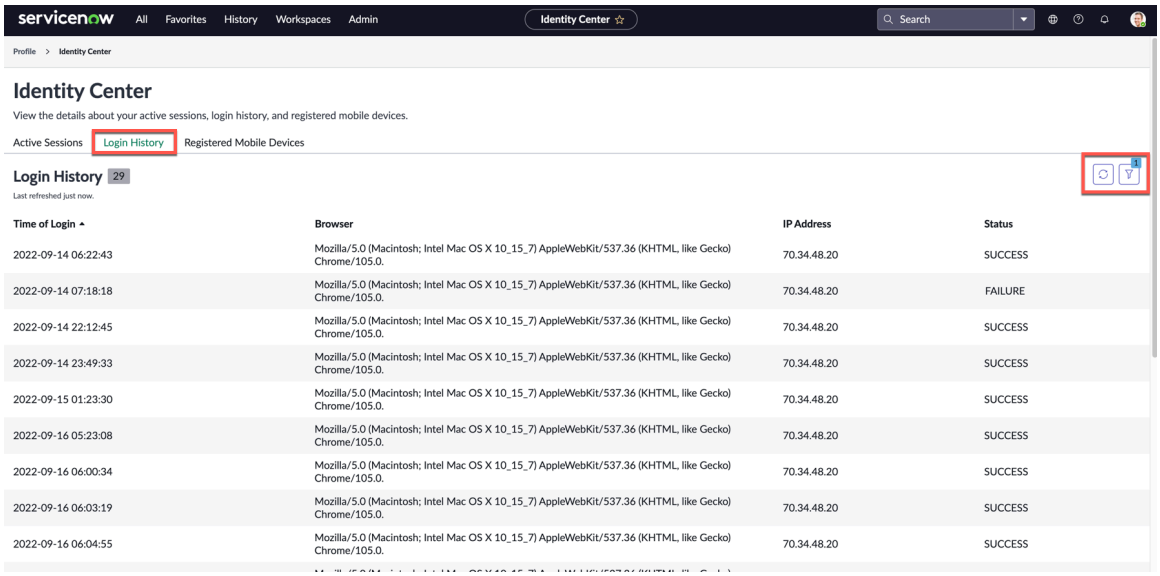
L'onglet Historique de connexion du Centre d'identité vous aide à obtenir vos informations de connexion et l'état de votre connexion.

Vous pouvez utiliser les filtres pour spécifier des actions de connexion afin de faciliter les enquêtes de sécurité. Le filtre peut vous aider à déterminer si l'activité était réelle ou suspecte et à signaler l'information à votre administrateur.

La pagination dans l'historique de connexion est de 20 par défaut et peut être définie sur un maximum de 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Voici quelques-uns des autres détails de l'historique de connexion :

- L'heure de connexion est l'heure de mise à jour à laquelle les équipements mobiles sont utilisés pour accéder à l'instance.
- Les enregistrements sont stockés dans Identity Center pendant 30 jours.

Affichage des équipements mobiles enregistrés dans Identity Center

Fournissez des détails sur votre mobile enregistré sur l'instance ServiceNow .

L'onglet Appareils mobiles enregistrés dans Identity Center affiche les détails de vos appareils enregistrés qui ont été utilisés pour accéder à l'instance ServiceNow .

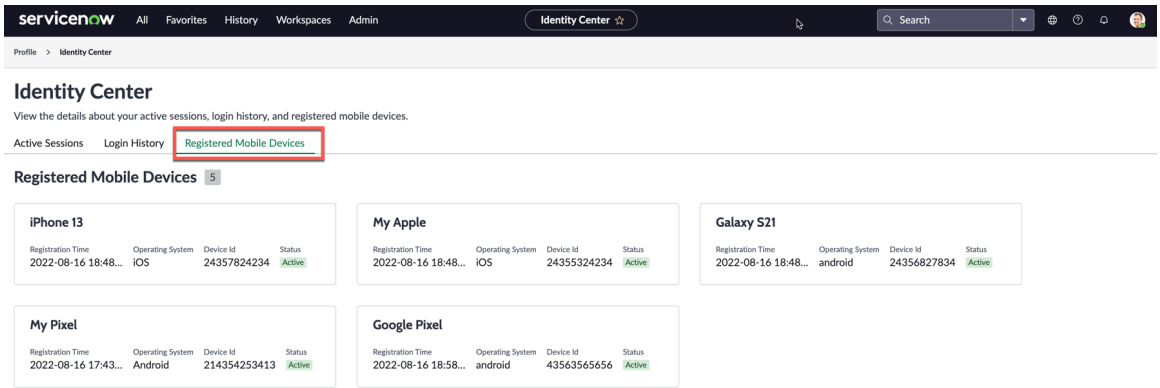
Si le module d'authentification adaptative est activé et qu'un équipement mobile enregistré est inscrit, Identity Center affiche les détails de vos appareils enregistrés.

En outre, il affiche également des détails sur les appareils, tels que le système d'exploitation, l'ID de l'appareil et l'état de l'appareil, ainsi que l'heure d'enregistrement de l'appareil.

Pour enregistrer votre équipement mobile, vous devez vous assurer que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) est installé et que vous avez activé votre fonctionnalité d'application mobile de confiance. Pour plus d'informations, consultez Activer l'application mobile de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Mesures d’identité pour les administrateurs

Affichez les tendances des utilisateurs, des utilisateurs privilégiés, des sessions actives et du compte intégré sur votre ServiceNow instance.

Mesures d’identité pour les administrateurs présente les tendances suivantes :

- Utilisateurs
- Utilisateurs privilégiés
- Comptes d’intégration ou non humains
- Sessions actives
- Sessions inactives

Pour en savoir plus, consultez les mesures du centre de sécurité.

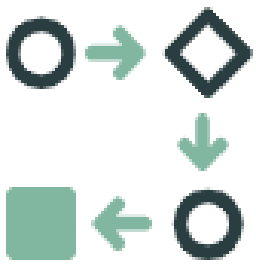
Console des identités des machines

Gérez vos comptes de services qui sont utilisés pour les intégrations avec ServiceNow.

Les identités machine sont des identités numériques qui interagissent avec les systèmes et les données. Ces identités sont utilisées pour effectuer des tâches de manière autonome. Machine Identity Console vous aide à comprendre le score de sécurité de ces identités et fournit des recommandations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer	Activer	Configurer
		
Découvrez les fonctionnalités et la valeur commerciale de Machine Identity Console.	Découvrez comment activer Machine Identity Console.	Configurez les intégrations entrantes à l'aide de la console d'identité de machine.

Traduction automatique

Exploration de la console d'identité de la machine

Gérez vos comptes de service, qui sont utilisés pour les intégrations avec ServiceNow.

Machine Identity Console vous permet de gérer vos identités non humaines (NHI) qui sont utilisées pour identifier, authentifier et autoriser différentes entités logicielles à accéder aux ressources sécurisées de ServiceNow. Les entités qui obtiennent l'accès comprennent les applications, les charges de travail, les API, les bots et les systèmes automatisés. Contrairement aux identités humaines, les identités non humaines (NHI) ne sont pas régies de la même manière et ne sont pas directement associées à un humain. Leur identité et leurs méthodes de vérification sont distinctes de celles des utilisateurs humains, et les mesures de sécurité humaine standard ne leur sont pas applicables.

https://player.vimeo.com/video/1101308622?h=b01d69f65a&badge=0&autopause=0&player_id=0&app_id=58479

Voici ce qui est disponible sur la page Vue d'ensemble de la console d'identité de machine :

- Total des comptes d'identité d'ordinateur (intégration) et comptes avec des rôles de privilège élevé.
- Appels d'API uniques : 7 derniers jours
- Méthode d'authentification utilisée : 7 derniers jours
- Score de sécurité de l'identité de la machine et résultats liés à l'identité.

Information associée

Activation de la console d'identité de machine

Résultats de sécurité

Mesures

Paramètres de la console d'identité de l'ordinateur

Intégrations entrantes

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations entrantes

Les intégrations entrantes dans la console d'identité de machine vous permettent de configurer et de gérer des applications externes pour accéder aux API ServiceNow.

Les intégrations entrantes dans la console d'identité des ordinateurs de ServiceNow vous aident à gérer et à configurer les intégrations et les applications qui se connectent à la plateforme ServiceNow. Il agit comme un concentrateur central pour stocker les paramètres de l'application et les informations d'identification de l'API, assurant ainsi une communication sécurisée entre ServiceNow et les systèmes externes. Pour en savoir plus, reportez-vous à la section Nouvelle expérience d'intégrations entrantes.

Types de connexions :

- OAuth : octroi du code d'autorisation : accédez à une ressource en vous authentifiant directement auprès d'un serveur OAuth qui lui fait confiance. Pour plus d'informations, consultez Configurer un octroi de code d'autorisation OAuth.
- OAuth : attribution d'informations d'identification du client : utilisée pour les intégrations entrantes d'un client OAuth tiers vers la plateforme ServiceNow. Pour plus d'informations, consultez Configurer une autorisation d'informations d'identification client OAuth.
- OAuth - Attribution titulaire JWT : utilisez une attribution de jeton Web JSON (JWT) pour vous authentifier auprès de votre instance. Pour plus d'informations, consultez Configurer une attribution de porteur de jeton Web JSON OAuth.
- Jeton d'ID tiers émis par le fournisseur d'identité prenant en charge OIDC : configurez un fournisseur OIDC OAuth pour accepter les jetons d'identité générés par un fournisseur OIDC tiers à l'aide d'appels d'API entrants. Pour plus d'informations, consultez Configurer un jeton d'ID de tiers.
- OAuth : attribution des informations d'identification du mot de passe de propriétaire de ressource : autorisez l'accès à un point de terminaison OAuth à l'aide d'un flux de code d'authentification. Pour plus d'informations, consultez Configurer un accord d'informations d'identification du mot de passe du propriétaire de ressource OAuth.

> **Remarque :**
> Pour le flux de code d'autorisation, l'utilisateur doit terminer l'authentification par connexion locale, SSO ou MFA, puis donner son consentement.

Pour en savoir plus, consultez .

Information associée

Intégrations entrantes

Configurer un octroi de code d'autorisation OAuth

Configurer une attribution de porteur de jeton Web JSON OAuth

Configurer un jeton d'ID de tiers

Configurer une autorisation d'informations d'identification client OAuth

Configurer un accord d'informations d'identification du mot de passe du propriétaire de ressource OAuth

Résultats de sécurité

Fournit le score de sécurité et les conclusions de l'identité de la machine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score et conclusions de sécurité de l'identité de la machine

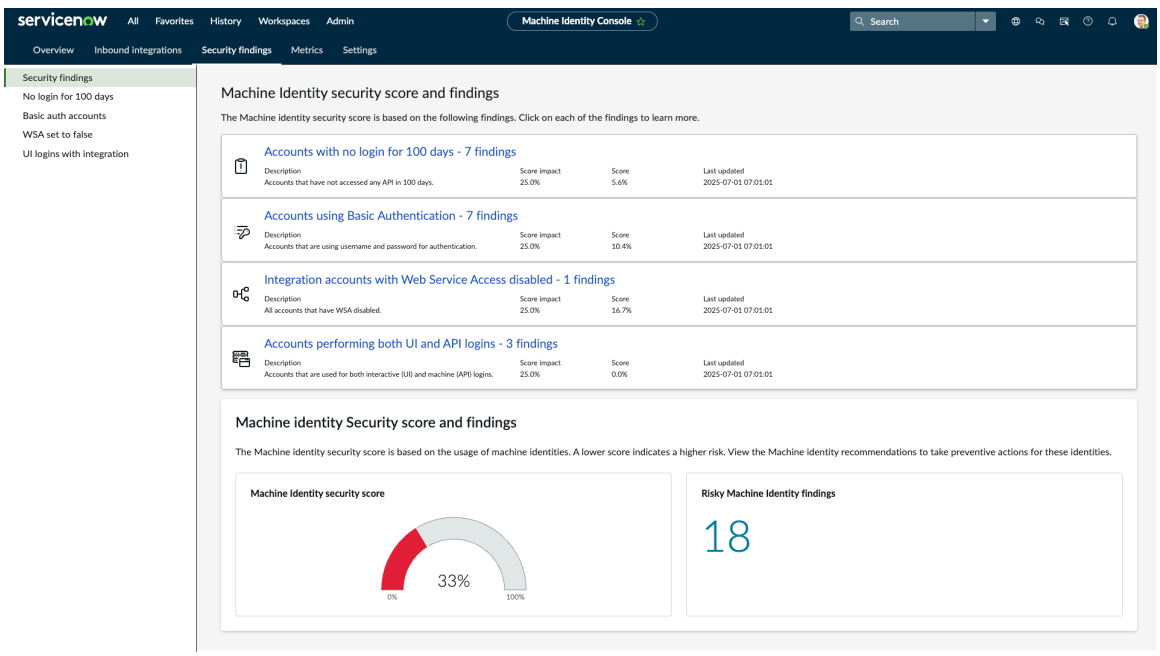
Le score de sécurité est affiché pour les résultats de sécurité suivants. Vous pouvez sélectionner chaque résultat pour en savoir plus.

Résultats de sécurité

Conclusions	Description
Comptes sans connexion depuis 100 jours	Résultats sur les comptes qui n'ont accédé à aucune API en 100 jours.
Comptes qui utilisent l'Authentification de base	Résultats sur les comptes qui utilisent le nom d'utilisateur et le mot de passe pour l'authentification.
Comptes d'intégration avec accès au service Web désactivé	Résultats sur tous les comptes pour lesquels WSA est désactivé.
Comptes exécutant à la fois des connexions via l'interface utilisateur et des connexions API	Résultats sur les comptes utilisés pour les connexions interactives (interface utilisateur) et machine (API).

Identité de la machine Score de sécurité et résultats

Le score de sécurité est basé sur l'utilisation et la méthode des identités des machines. Un score inférieur indique un risque plus élevé. Vous pouvez consulter les recommandations de mesures préventives pour ces identités.



Comptes sans connexion depuis 100 jours

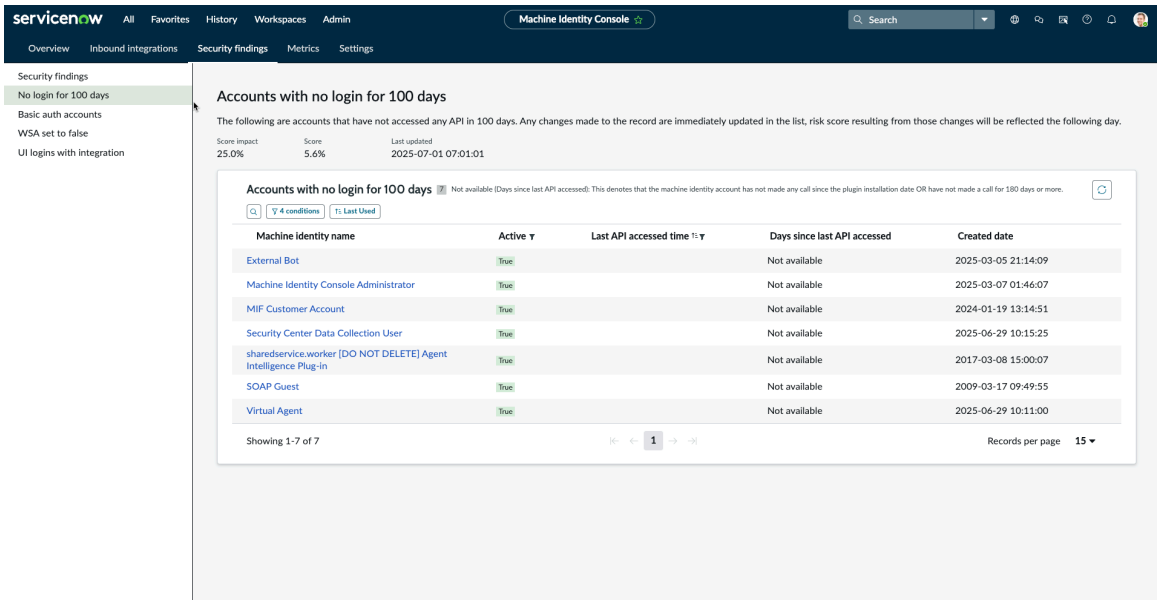
Affichez les résultats sur les comptes qui n'ont accédé à aucune API en 100 jours sous les résultats de sécurité dans la console d'identité de machine.

Comptes sans connexion pendant 100 jours affiche les comptes d'identité non humaine qui n'ont accédé à aucune API en 100 jours.

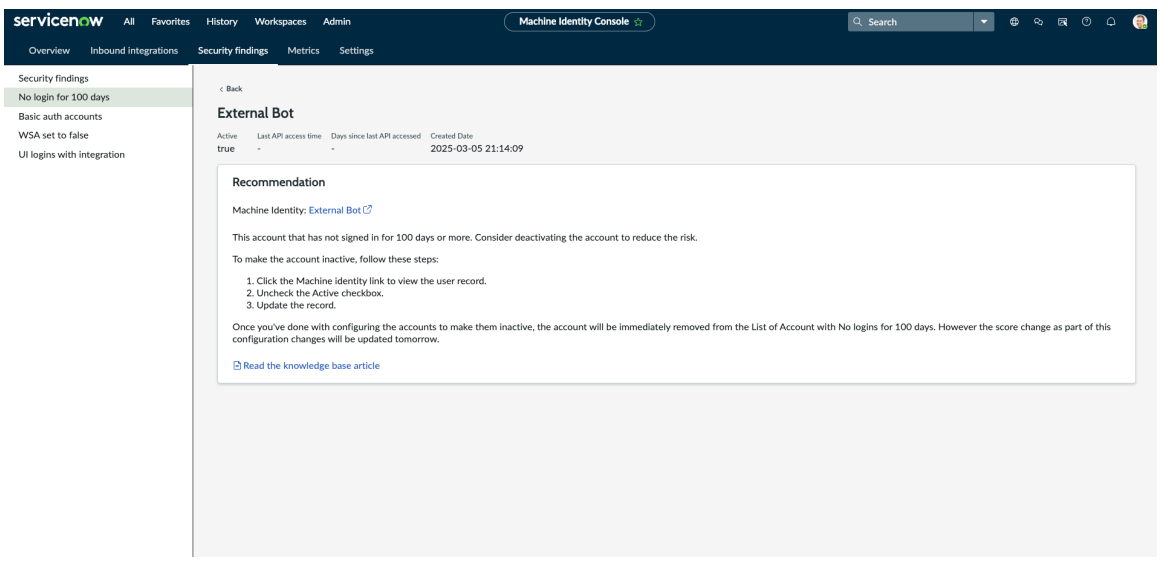
Remarque :
Tous les changements apportés à l'enregistrement affiché sur cette page sont immédiatement mis à jour dans la liste. Le score de risque résultant de ces changements est reflété le lendemain.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez sélectionner le nom de l'identité de machine pour en savoir plus sur le compte et la recommandation pour maintenir une bonne posture de sécurité pour le compte.



Comptes qui utilisent l'Authentification de base

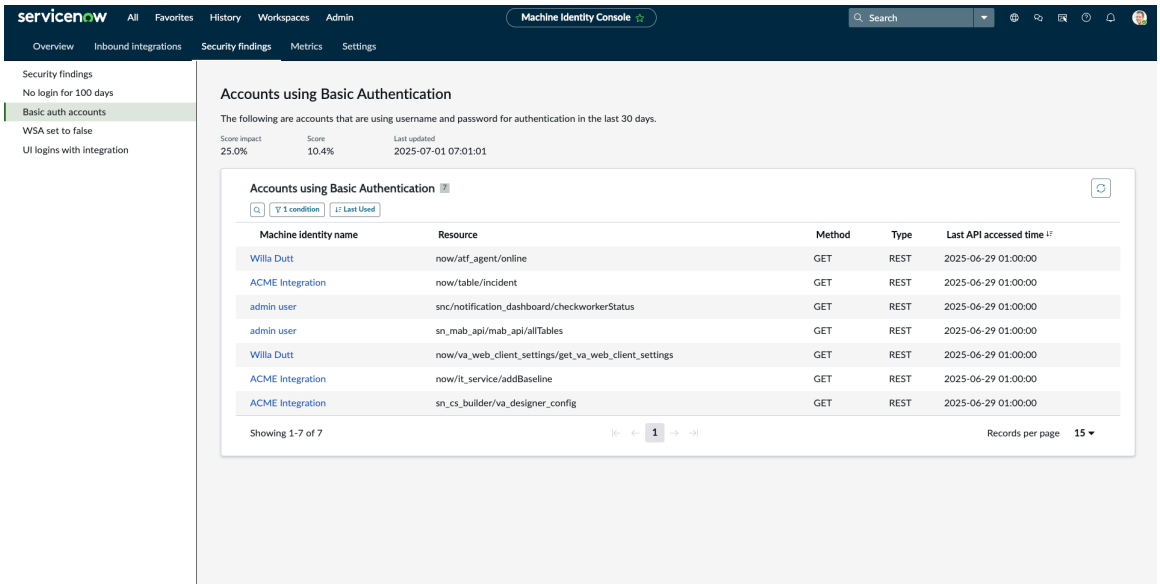
Affichez les résultats sur les comptes qui utilisent uniquement l'authentification de base pour authentifier les API sous les résultats de sécurité dans la console d'identité de machine.

Comptes utilisant l'authentification de base affiche les comptes d'identité non humaine qui utilisent l'authentification de base pour les API pour se connecter à ServiceNow.

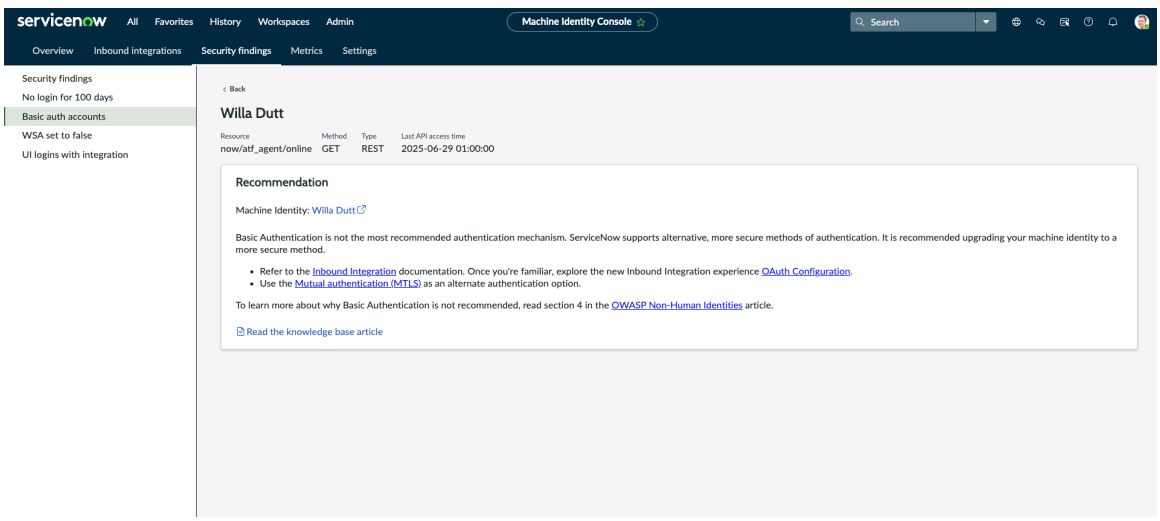
Remarque :
Les comptes affichés sur la page sont les comptes qui utilisent le nom d'utilisateur et le mot de passe pour l'authentification au cours des 30 derniers jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez sélectionner le nom de l'identité de machine pour en savoir plus sur le compte et la recommandation pour maintenir une bonne posture de sécurité pour le compte.



Comptes d'intégration avec accès au service Web défini sur faux

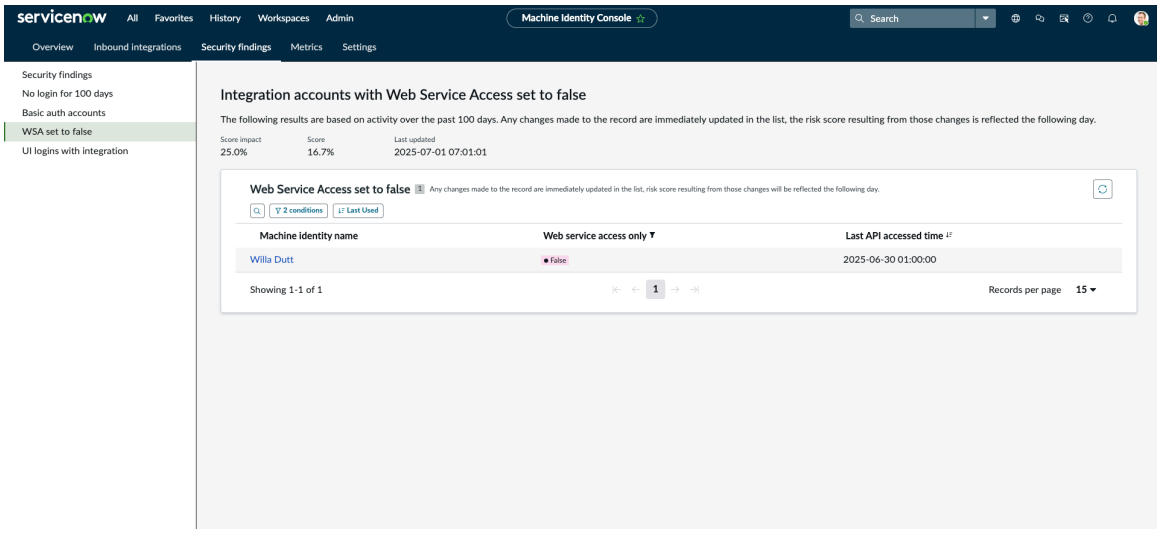
Affichez les résultats sur les comptes qui font l'authentification ServiceNow avec l'accès au service Web défini sur faux sous les résultats de sécurité dans la console d'identité de la machine.

Comptes d'intégration dont l'accès au service web est défini sur faux affiche les comptes qui utilisent l'API sans que l'accès au service web soit défini sur faux.

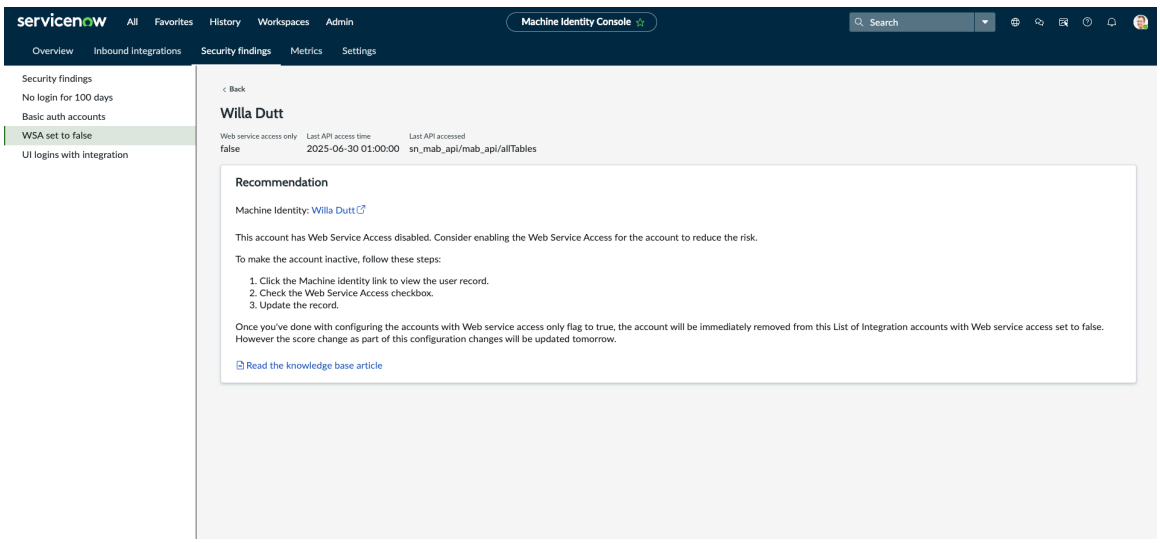
Remarque :
Tous les changements apportés à l'enregistrement affiché sur cette page sont immédiatement mis à jour dans la liste. Le score de risque résultant de ces changements est reflété le lendemain.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez sélectionner le nom de l'identité de machine pour en savoir plus sur le compte et la recommandation pour maintenir une bonne posture de sécurité pour le compte.



Comptes effectuant à la fois la connexion à l'interface utilisateur et à l'API

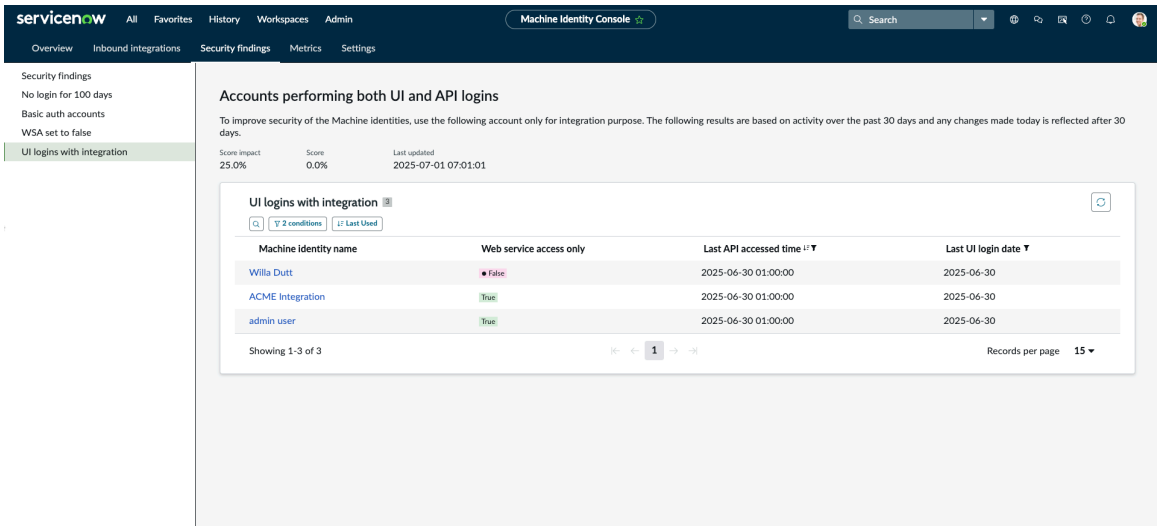
Affichez les résultats sur les comptes qui effectuent la connexion à l'interface utilisateur et à l'API sous les résultats de sécurité dans la console d'identité de la machine.

Les comptes effectuant à la fois la connexion à l'interface utilisateur et à l'API affichent les comptes qui utilisent la connexion à l'interface utilisateur et à l'API pour s'authentifier auprès de ServiceNow.

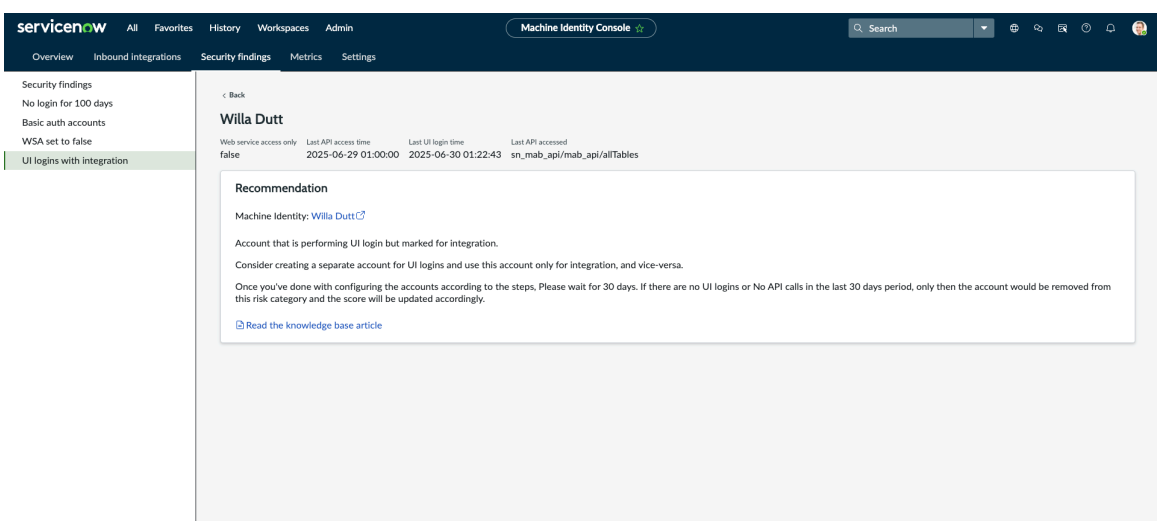
Remarque :
Les comptes affichés sur la page sont basés sur l'activité au cours des 30 derniers jours et tout changement apporté aujourd'hui est reflété après 30 jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez sélectionner le nom de l'identité de machine pour en savoir plus sur le compte et la recommandation pour maintenir une bonne posture de sécurité pour le compte.



Mesures

Mesures des identités des ordinateurs.

Appels d'API uniques au cours des 7 derniers jours

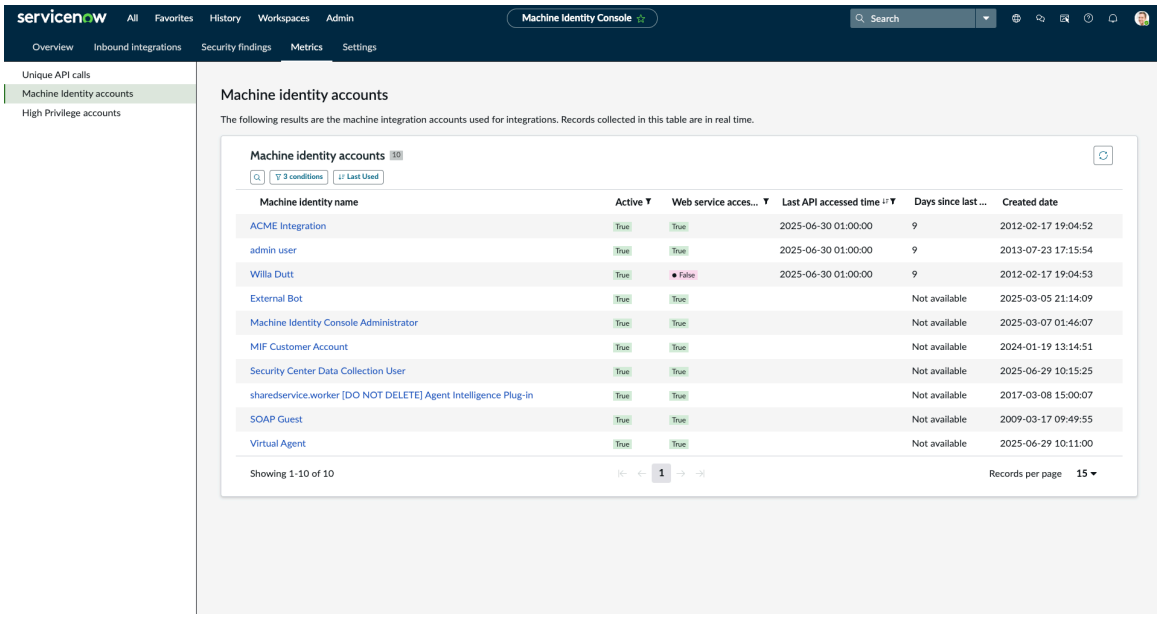
Les résultats suivants sont des appels d'API uniques au cours des 7 derniers jours. Les enregistrements collectés dans cette table le sont en temps réel.

Comptes d'identité de machine

Les résultats suivants correspondent aux comptes d'intégration de machine utilisés pour les intégrations. Les enregistrements collectés dans cette table le sont en temps réel.

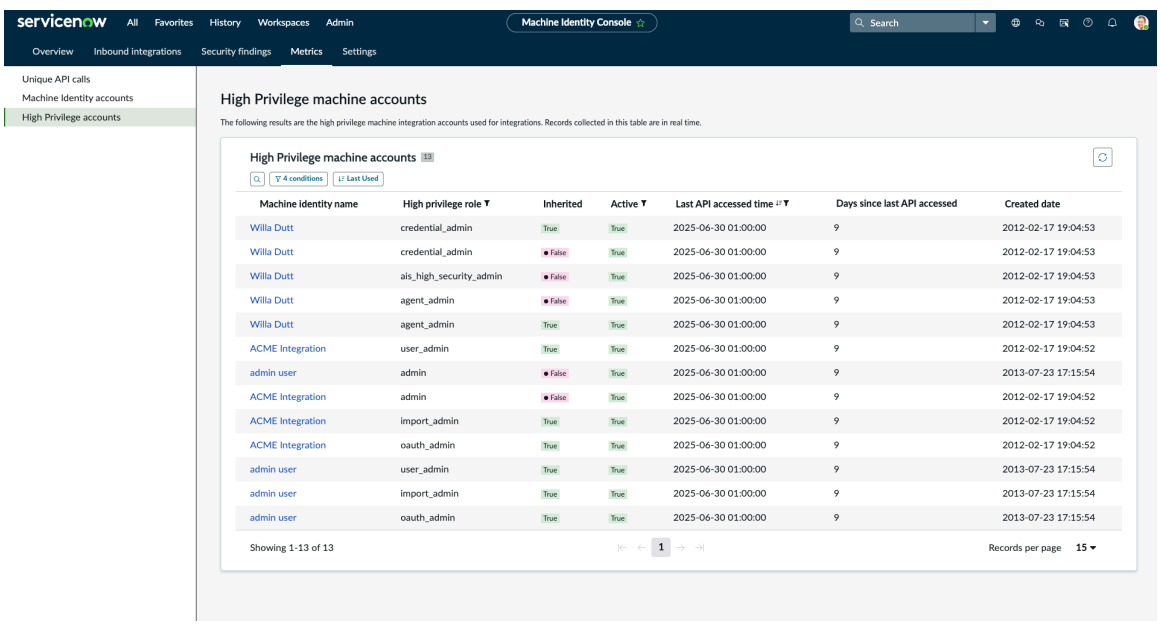
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comptes de machines à privilèges élevés

Les résultats suivants correspondent aux comptes d'intégration de machine à privilège élevé utilisés pour les intégrations. Les enregistrements collectés dans cette table le sont en temps réel.



Paramètres de la console d’identité de l’ordinateur

Configurez les paramètres de score de sécurité de l’identité de la machine.

Avant de commencer

Rôle requis : mi_admin

La tâche suivante est spécifique à votre organisation sur la façon de gérer les comptes inactifs.

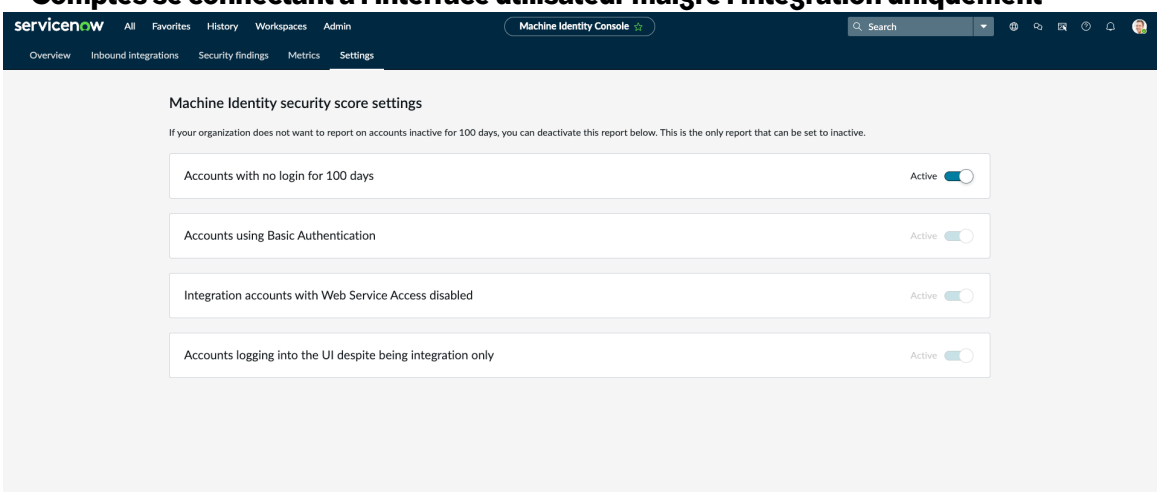
Remarque :
Si votre organisation ne souhaite pas générer de rapports sur les comptes inactifs pendant 100 jours, vous pouvez désactiver ce rapport ci-dessous. Il s’agit du seul rapport qui peut être défini comme inactif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Console des identités des machines** > **Paramètres**.
2. Sélectionnez les paramètres en fonction de vos besoins :
   - **Comptes sans connexion depuis 100 jours**
   - **Comptes qui utilisent l'Authentification de base**
   - **Comptes d'intégration avec accès au service Web désactivé**
   - **Comptes se connectant à l'interface utilisateur malgré l'intégration uniquement**



Activation de la console d’identité de machine

Activez la com.glide.identity.machine_identity_management **Gestion de l’identité de machine** pour gérer vos comptes de services qui sont utilisés pour les intégrations avec ServiceNow.

Avant de commencer

Rôle requis : mi_admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d’extension **Gestion de l’identité de machine** (com.glide.identity.machine_identity_management) à l’aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d’informations sur les composants installés avec un module d’extension, voir Rechercher les composants installés avec une application .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de la console d’identité de la machine

Gérez vos comptes de service qui sont utilisés pour les intégrations avec ServiceNow à l’aide de la console d’identité de machine.

Avant de commencer

Rôle requis : mi_admin

Activez le module d’extension**Gestion de l’identité de la machine** com.glide.identity.machine_identity_management. Pour plus d'informations, consultez Activation de la console d’identité de machine.

Procédure

1. Accédez à la **Tous** > **Console des identités des machines** > **Console des identités des machines**.
   La console d’identité de machine comporte les onglets suivants :
   - Vue d’ensemble : affiche l’ensemble des comptes d’identité de machine et leurs mesures
   - Intégrations entrantes: configurez les intégrations entrantes pour les API.
   - Résultats de sécurité: affiche que le score de sécurité est basé sur différents résultats de sécurité.
   - Mesures: affiche les différentes mesures des comptes d’identité d’ordinateur
   - Paramètres : configurez la console d’identité de la machine.
2. Sélectionnez les onglets appropriés en fonction de vos besoins de sécurité.

Système de gestion des identités interdomaines (SCIM)

L’API SCIM (System for Cross-domain Identity Management) fournit des points de terminaison pour créer, lire, mettre à jour et supprimer des opérations sur des utilisateurs et des groupes à l’aide du protocole SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fournisseur SCIM



Le fournisseur SCIM synchronise les changements apportés aux identités dans le fournisseur d'identités, y compris la création, la mise à jour ou la suppression d'enregistrements.

Client SCIM



Le client SCIM est utilisé pour créer, mettre à jour et supprimer des ressources d'identité dans un système qui prend en charge les demandes REST compatibles SCIM.

Traduction automatique

Le protocole SCIM est un protocole basé sur HTTP au niveau de l'application et basé sur la norme HTTP (RFC7230). Utilisez cette API pour la mise en service et la gestion des données d'identité, telles que les utilisateurs et les groupes. Utilisez l'API sur le Web et dans des environnements interdomaines, tels que des fournisseurs de services de l'entreprise au cloud ou des scénarios intercloud.

Pour accéder à cette API, vous devez activer le module d'extension SCIM v2 - ServiceNow® Cross-domain Identity Management (com.snc.integration.scim2).

Pour en savoir plus sur l'API SCIM, consultez API System for Cross-domain Identity Management .

Fournisseur SCIM

Le fournisseur de services met en service des utilisateurs et des groupes à l'aide de l'API SCIM.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



En savoir plus sur le fournisseur SCIM.

Activer



Activez SCIM.

Personnalisation SCIM



Obtenez des détails sur la personnalisation de SCIM.

Définition de la source



En savoir plus sur la définition de source pour SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration du fournisseur SCIM

Le fournisseur de services met en service des utilisateurs et des groupes à l'aide de l'API SCIM.

En tant que fournisseur SCIM, les ServiceNow schémas prennent en charge les API SCIM pour mettre en service les utilisateurs et les groupes.

Le fournisseur SCIM synchronise les changements apportés aux identités dans le fournisseur d'identités, y compris la création, la mise à jour ou la suppression d'enregistrements. Ces modifications sont automatiquement synchronisées avec le fournisseur selon le protocole SCIM. En outre, l'IdP peut lire les identités du fournisseur pour les ajouter au répertoire IdP. L'IdP peut alors détecter des valeurs incorrectes dans le fournisseur qui pourraient créer des failles de sécurité. La synchronisation permet aux utilisateurs finaux d'avoir un accès transparent aux applications pour lesquelles ils sont affectés, avec des profils et des autorisations à jour.

Configurations du fournisseur SCIM

Pour configurer le fournisseur SCIM, procédez comme suit :

- Activez le module **d'extension SCIM v2 - Gestion des identités interdomaines ServiceNow** . Pour en savoir plus, reportez-vous à la section Activer le module d'extension SCIM.
- Activez les autres modules d'extension que les autres modules d'extension requis pour SCIM :
  - OAuth 2.0
  - Fournisseur d'API REST
  - Politique d'accès REST API
- Ajoutez le rôle scim_admin dans le cadre du service SCIM.

> **⚠ Avertissement :**
> Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où l'scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Tables

Deux tables, sys_user et sys_group, contiennent les attributs SCIM qui ne sont pas mappés aux tables existantes ServiceNow . Pour en savoir plus sur les tables, consultez les tables spécifiques à SCIM .

Activer le module d'extension SCIM

Pour l'activation de SCIM, installez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2).

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Recherchez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2) à l'aide des critères de filtre et de la barre de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Didacticiel : Configurer SCIM pour l'attribution d'utilisateurs avec un fournisseur

La configuration de SCIM met automatiquement en service et déprovisionne les utilisateurs et les groupes ServiceNow à l'aide du service de mise en service des fournisseurs.

Avant de commencer
Installez le module d'extension SCIM.

Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où l'scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Pourquoi et quand exécuter cette tâche
Vous pouvez mettre en service des utilisateurs à l'aide de SCIM à l'aide des méthodes d'authentification suivantes :

- Mise en service de l'utilisateur à l'aide de l'authentification de base
- Mise en service d'un utilisateur à l'aide d'OAuth

Mise en service de l'utilisateur à l'aide de l'authentification de base

La configuration de SCIM met en service et annule automatiquement la mise en ServiceNow service des utilisateurs et des groupes à l'aide du service de mise en service des fournisseurs avec authentification de base.

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où l'scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Vous devez activer le module d'extension SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API** pour vérifier les détails des politiques d'accès de l'API REST.
2. Sur la page Politique d'accès API, cliquez sur l'enregistrement **Politique d'API SCIM** .
3. Vérifiez que l'enregistrement **Authentification de base de l'API SCIM** est disponible dans les sections Profils d'authentification.
4. Sélectionnez **Authentification de base** comme type.
5. Créez les configurations requises du côté du fournisseur.
6. Testez la connexion pour vous assurer que le fournisseur peut se connecter à ServiceNow.

Remarque :
Si la connexion échoue, assurez-vous que votre ServiceNow compte dispose des autorisations d'administrateur et réessayez.

Mise en service d'un utilisateur à l'aide d'OAuth

Configurez le fournisseur pour la mise en service et l'annulation de l'approvisionnement automatiques des utilisateurs et des groupes ServiceNow pour SCIM à l'aide du service de mise en service du fournisseur avec OAuth.

Avant de commencer

Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où l'scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Vous devez activer le module d'extension SCIM.

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
2. Dans la page Registres d'application, cliquez sur l'enregistrement de **l'API SCIM** .
3. Vérifiez les détails de l'enregistrement de **l'API SCIM** .

   Ces détails doivent être fournis lors de la configuration de l'application ServiceNow sur Azure AD.
4. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API** pour vérifier les détails des politiques d'accès de l'API REST.
5. Sur la page Politique d'accès API, cliquez sur l'enregistrement **Politique d'API SCIM** .
6. Vérifiez que l'enregistrement **SCIMAPIOAuthOnly** est disponible dans les sections Profils d'authentification.
7. Vérifiez si le champ **Entité OAuth** est spécifié avec l'enregistrement **d'API SCIM** précédemment configuré ou vérifié en tant que registre d'application.
8. Créez les configurations requises du côté du fournisseur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Testez la connexion pour vous assurer que le fournisseur peut se connecter à ServiceNow.

> **Remarque :**
> Si la connexion échoue, assurez-vous que votre ServiceNow compte dispose des autorisations d'administrateur et réessayez.

Dépannage SCIM

Scénarios d'erreur courants lors de l'intégration à SCIM.

URL de l'API REST non valide

Action : entrez une URL d'API valide. Pourra vérifier l'URL de l'API **REST dans l'explorateur d'API REST**.

Aucune URL de redirection n'est définie dans l'instance ServiceNow

Action : saisissez une URL de redirection valide pour l'entité OAuth SCIM dans ServiceNow. Entrez l'URL de redirection lors de la configuration de l'entité OAuth dans ServiceNow.

Lorsque l'URL de redirection est différente de la requête

Action : « **redirect_url** » fournie dans « Point de **terminaison d'autorisation »** doit être identique à l'entité OAuth configurée dans ServiceNow.

> **Remarque :**
>
> Cette erreur se produit en cas d'incompatibilité entre Azure « Point de terminaison d'autorisation » et ServiceNow « URL de redirection »

Lorsqu'un secret client non valide est transmis

Action : la valeur saisie dans « Secret client » doit être identique à l'entité OAuth configurée dans ServiceNow.

Lorsqu'un « ClientId » non valide est transmis dans le « Point de terminaison d'autorisation » Azure

Action : la valeur saisie pour le paramètre « client_id » dans « Point de terminaison d'autorisation » doit être identique à l'entité OAuth configurée dans ServiceNow.

Personnalisation SCIM

Personnalisez les protocoles SCIM pour votre gestion des identités.

La personnalisation SCIM vous permet d'effectuer les opérations suivantes :

- Prenez en charge les champs personnalisés sur les tables sys_user et sys_user_group via la génération de schémas d'extensions dynamiques.
- Offrir la possibilité de remplacer les mappages SCIM par défaut.

Un administrateur SCIM peut définir des schémas d'extension personnalisés pour les ressources d'utilisateur et de groupe. Les attributs définis dans le schéma d'extension personnalisé peuvent être mappés aux champs des tables sys_user ou sys_user_group.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations de la personnalisation SCIM

Pour la personnalisation SCIM, vous devez effectuer les tâches suivantes :

- Définissez un schéma d'extension personnalisé pour les utilisateurs et les groupes dans la table Schéma d'extension SCIM. Pour plus d'informations, Créer un schéma d'extension SCIM reportez-vous à la section .
- Créez des entités dans une définition ETL pour les attributs de schéma personnalisés. Les entités sont créées pour la table cible mappée avec les attributs sys_user ou sys_user_group. Pour plus d'informations, reportez-vous à la section Créer une définition SCIM ETL.
- Créez un mappage RTE entre ces deux entités. Pour plus d'informations, reportez-vous à l'étape 5 de la section Créer une définition SCIM ETL.
- Envoyer des attributs de schéma personnalisé avec des données dans la charge utile de la demande d'API SCIM.

L'API SCIM appelle le moteur RTE avec le mappage défini. Les données sont stockées dans les champs respectifs de la table cible, tel que défini dans le mappage.

Propriétés et schémas de personnalisation SCIM

La personnalisation SCIM inclut les propriétés, schémas pris en charge et schémas non pris en charge suivants.

Propriétés

La personnalisation SCIM ajoute les propriétés système suivantes.

Propriétés

Nom	Description
com.snc.integration.scim2.max.member.count	Nombre maximal de membres SCIM.
com.snc.integration.scim2.resolve.external.conflict	Résoudre les conflits SCIM en fonction de la définition de source du client demandeur si des ressources multiples sont trouvées avec un filtre SCIM d'ID externe. **Remarque :** En tant que condition préalable, si la mise en service est effectuée à partir de plusieurs sources, les sources doivent être définies dans la table Définition de source SCIM. Si les sources ne sont pas définies ou si cette propriété est inactive, toutes les ressources correspondantes sont renvoyées avec une réponse de filtre d'ID externe.
com.snc.integration.scim2.user.etl.definition.id	ID de définition ETL de l'utilisateur SCIM.
com.snc.integration.scim2.group.etl.definition.id	ID de définition ETL du groupe SCIM.
com.snc.integration.scim2.rte.verbose.logging.enabled	Activer la journalisation détaillée pour les définitions RTE d'utilisateur et de groupe SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
com.snc.integration.scim2.string.field_length_validation.enabled	Validation de la longueur des champs. Cette propriété active la validation au lieu de tronquer et d'enregistrer le champ.
com.snc.integration.scim2.provider.custom_id	ID de l'action de script pour la personnalisation des réponses SCIM.

Schémas pris en charge

La personnalisation SCIM ajoute les schémas pris en charge suivants.

Schémas pris en charge

Schémas	Description	Préfixe	Exemple
urn:ietf:params:scim:schemas:core:2.0:User	Inclut les attributs de base pour les ressources.	*urn:ietf:params:scim:schemas:core:2.0:User*	nom.deuxième prénom
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Inclut les attributs associés à ServiceNow.	*urn:ietf:params:scim:schemas:extension:servicenow:2.0:User*	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User	Inclut les attributs personnalisés qui ne sont pas mappés dans le cadre de l'extension principale ou du schéma d'extension ServiceNow .	*urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User*	ID_social personnalisé

Schéma non pris en charge

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: comprend les attributs couramment utilisés pour représenter les utilisateurs qui appartiennent à une entreprise ou à une entreprise ou agissent en son nom.

Remarque :
Le schéma Enterprise est un schéma valide, mais ses attributs sont mappés à n'importe quelle table. La persistance de la base de données n'étant pas prise en charge, aucune erreur ne s'affiche si un schéma d'entreprise est inclus dans le corps de la demande.

Créer un schéma d'extension SCIM

Créez des attributs personnalisés à mapper sur des champs qui ne sont pas mappés dans le cadre du schéma de base ou du schéma d'extensions ServiceNow .

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables qui peuvent contourner la logique métier ou la protection ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

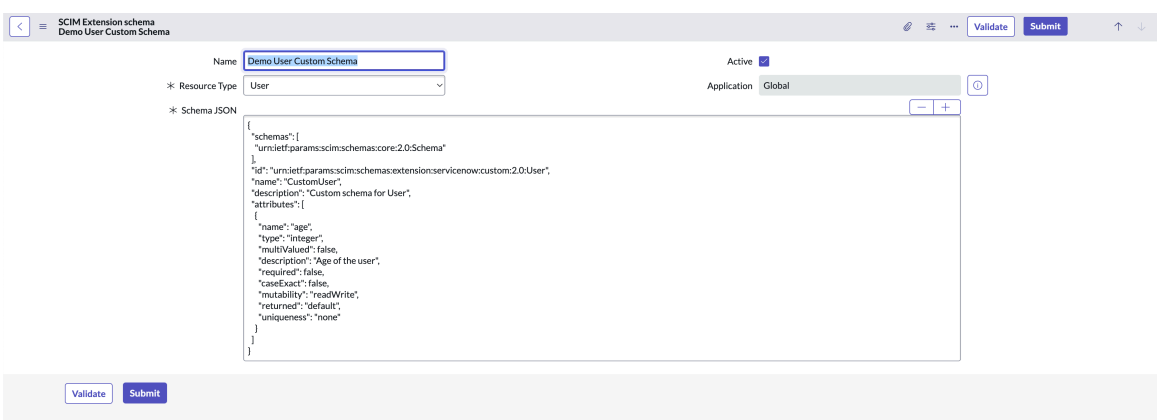
Procédure

1. Accédez à la **Tous** > **SCIM** > **Schémas d'extension SCIM**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

> **Remarque :**
> Un seul schéma d'extension peut être mappé au champ **Type de ressource** . Par exemple, Utilisateur en tant que type de ressource peut être mappé à un schéma d'extension utilisateur.

Schéma d'extension SCIM

Champ	Description
Nom	Nom du schéma des extensions.
Actif	Option permettant d'activer le schéma. Sélectionnez ce champ si l'enregistrement doit être considéré comme un schéma d'extension personnalisé. Un seul enregistrement de schéma d'extension personnalisé peut être actif à la fois pour un type de ressource spécifique, que ce soit pour le type Utilisateur ou Groupe.
Type de ressource	Type de ressource qui doit être mappé au schéma des extensions. Les options sont les suivantes : ○ **Utilisateur** ○ **Groupe**
Application	Le périmètre de l'application pour cet enregistrement.
JSON de schéma	Détails dans les schémas JSON. Pour plus d'informations sur la définition du schéma d'extension avec des attributs, consultez Datatracker .



4. Validez les attributs en cliquant sur **Valider**.
5. Cliquez sur **Envoyer**.

Résultats

Le schéma des extensions avec des attributs personnalisés associés au type de ressource Utilisateur ou Groupe est créé. Utilisez les définitions SCIM ETL pour mapper les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ressources en fonction du schéma d'extension dans la table sys_user et sys_user_group. Pour plus d'informations, consultez Créer une définition SCIM ETL.

Créer une définition SCIM ETL

Utilisez les définitions SCIM ETL pour mapper les attributs personnalisés aux tables sys_user ou sys_user_group.

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables qui peuvent contourner la logique métier ou la protection ACL.

Remarque :

- Les définitions ETL de groupe SCIM et d'utilisateur SCIM font partie du système de base pour le mappage des ressources. Vous pouvez utiliser les mêmes mappages de ressources et modifier les critères selon vos besoins, ou créer de nouveaux mappages de ressources.
- Les champs [*] ne sont pas pris en charge via RTE dans le mappage SCIM.

Procédure

1. Suivez les instructions de la section Créer des définitions ETL (Extraire/Transformer Charger).
2. Ouvrez l'enregistrement nouvellement créé et affichez les détails.
3. Dans la section Entités ETL, créez une entité en cliquant sur **Nouveau**.
   Vous devez créer des entités pour les utilisateurs suivants :
   - scim-user : pour les champs qui proviennent de SCIM.
   - Table d'utilisateur (sys_user) ou de groupe (sys_user_group) : pour les champs que vous souhaitez mapper à partir de la table de base de données avec SCIM. Par exemple, pour personnaliser les détails de l'utilisateur via SCIM, vous pouvez utiliser la table sys_user.

   a. Remplissez les champs du formulaire.

Formulaire d'entité ETL

Champ	Description
Nom	Nom de l'entité ETL.
Application	Le périmètre de l'application pour cet enregistrement.
Table	Table cible pour l'entité ETL.
Définition	Entité ETL sélectionnée.
Chemin d'accès	Chemin d'accès unique pour cette entité. Ne spécifiez aucun chemin d'accès pour l'entité représentant la table de jeux d'importation. Lorsqu'une entité représente une collection, le chemin d'accès doit se terminer par un astérisque

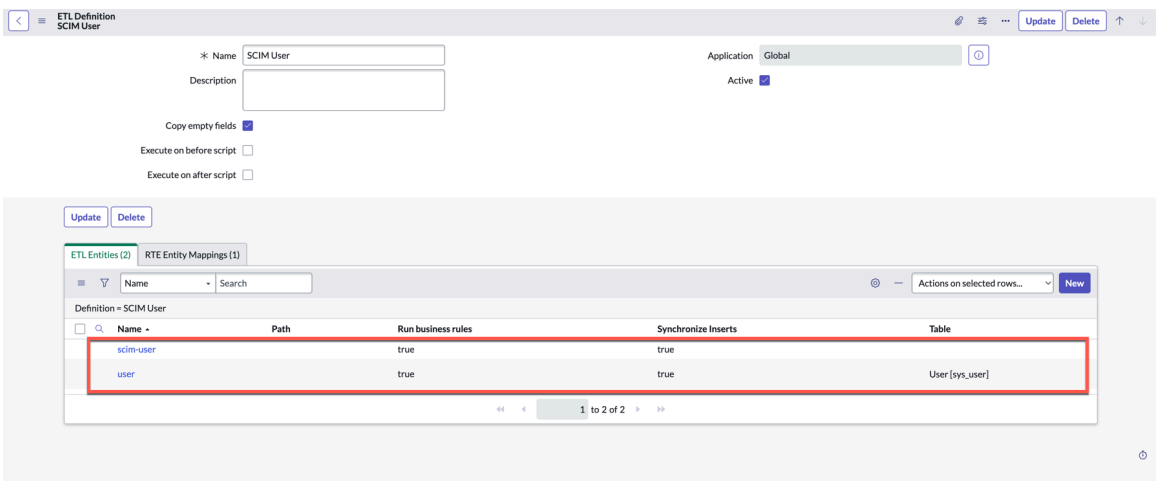
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	[*]. Cette exigence s’applique aux entrées intermédiaires et à l’entité de table cible.
Synchroniser les insertions	Option permettant de garantir uniquement un enregistrement avec des valeurs de champ fusionnées uniques en synchronisant les insertions d’enregistrement.
Exécuter les règles métier	Option permettant d’exécuter des règles métier.

b. Cliquez sur **Envoyer**.

Les entités ETL sont créées pour les tables scim-user et user. Vous devez créer des champs d’entité ETL au sein de ces entités ETL et mapper les deux entités en créant un mappage d’entité RTE.



4. Créez les entités et mappez-les.

a. Ouvrez l’enregistrement soumis (utilisateur scim et utilisateur).

b. Dans les champs Entité ETL, ajoutez les champs en cliquant sur **Nouveau**.

c. Remplissez les champs du formulaire.

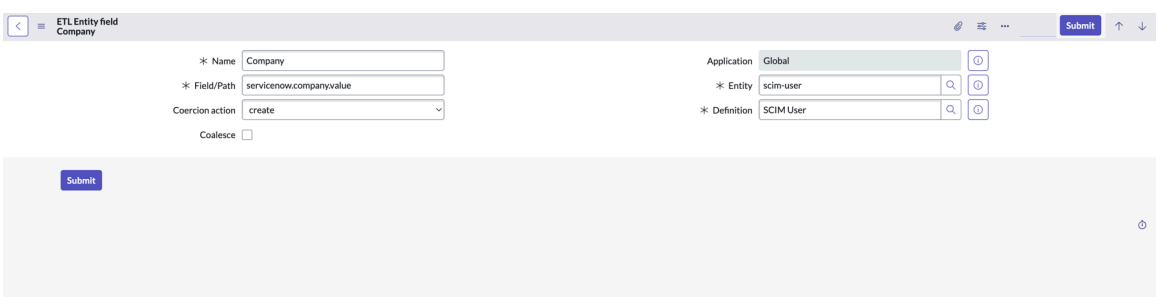
Formulaire d’entité ETL

Champ	Description
Nom	Nom de la définition de champ de l’entité ETL.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ/chemin d'accès	Ce champ est soit une colonne, soit un chemin d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Le champ est un nom de colonne lorsque l'entité est la table d'importation ou la table cible. ▪ Le champ est un chemin d'accès lorsque le champ possède des structures imbriquées.
Entité	Entité à laquelle cette opération s'applique. Choisissez l'entité à l'aide de l'icône de recherche.
Action de forçage	Ce que le système doit faire si une référence ou un choix n'a pas pu être trouvé. Les options sont les suivantes : ▪ **Créer** : créez une nouvelle référence ou un nouveau choix. Affectez la référence ou le choix à l'enregistrement actuel. ▪ **Rejeter** : ne pas enregistrer l'enregistrement entier dans la base de données. ▪ **Ignorer** : définir la valeur actuelle comme vide.
Définition	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Fusion	Option permettant d'interroger les enregistrements existants.



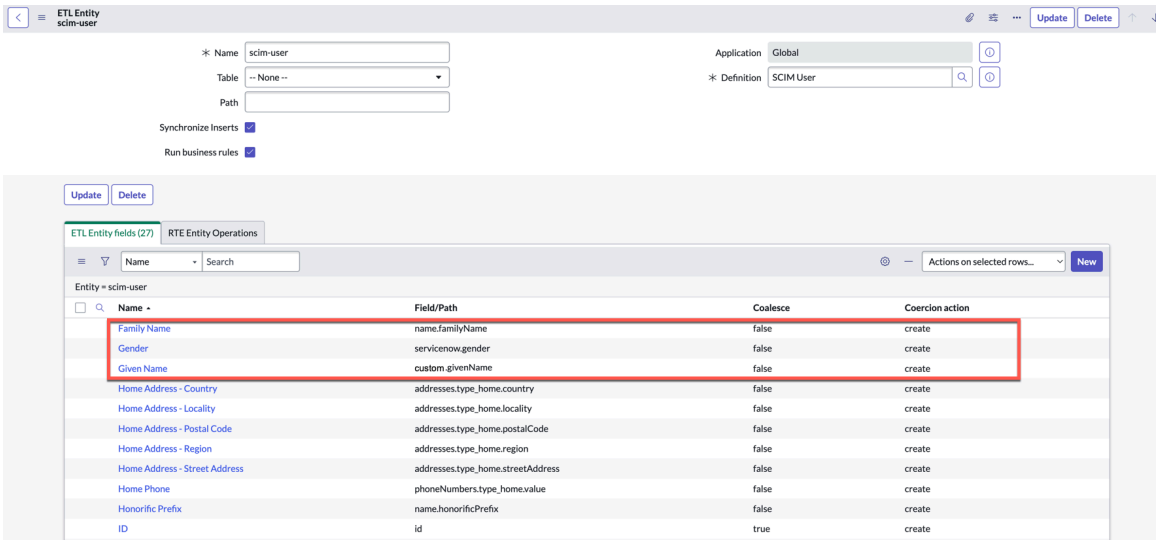
d. Soumettez les entrées en cliquant sur **Soumettre**.

Vous pouvez ajouter plusieurs entrées en tant que champ Entité ETL en fonction de vos besoins.

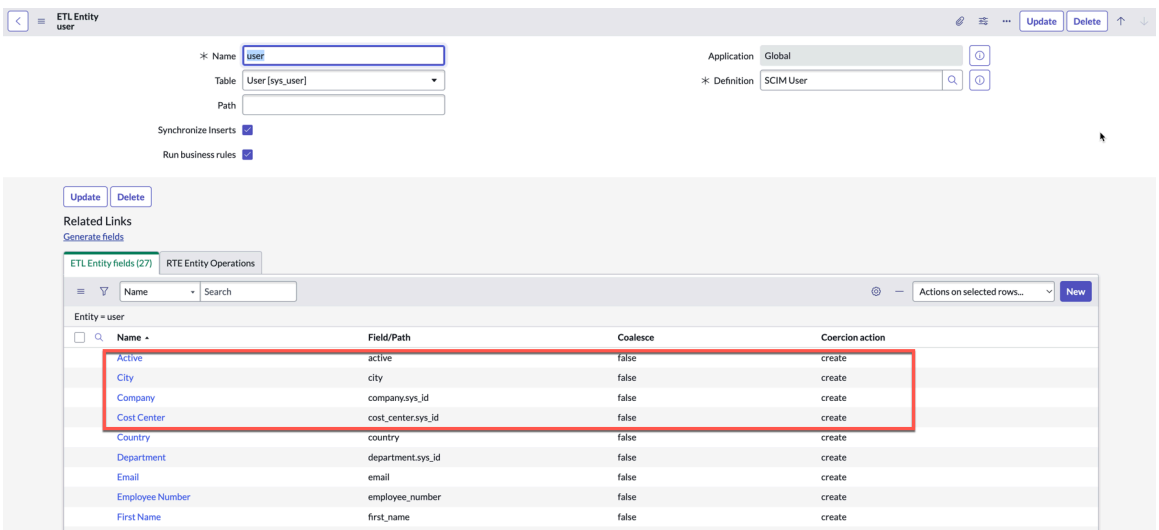
L'entité ETL scim-user peut avoir des entités avec l'extension principale (user), l'extension ou l'extension ServiceNow personnalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'entité ETL utilisateur peut avoir des entités de la table de base de données. Par exemple, sys_user table.



Remarque :
Pour ajouter un filtre dans les champs SCIM entrants, utilisez un trait de soulignement (_). Ce trait de soulignement se traduit par un filtre d'égalisation. Par exemple, l'attribut `email.type_work.value` applique le filtre SCIM de l'e-mail `[type eq "work"].value`.

Une fois les champs créés dans les enregistrements d'entité SCIM-user et ETL d'utilisateur, vous devez créer un enregistrement de mappage d'entité RTE. Vous devez ensuite spécifier la définition source et la définition cible pour mapper les deux champs.

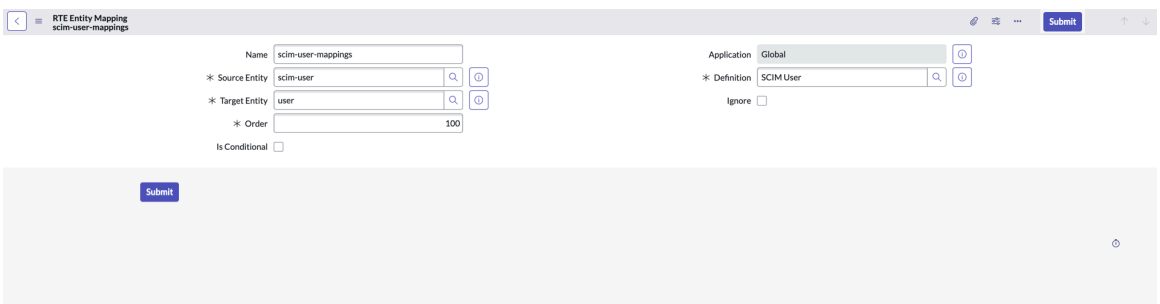
5. Dans la section Mappages d'entités RTE, créez un mappage d'entité en cliquant sur **Nouveau**
6. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du mappage.
Entité source	Entité source pour le mappage.

Traduction automatique

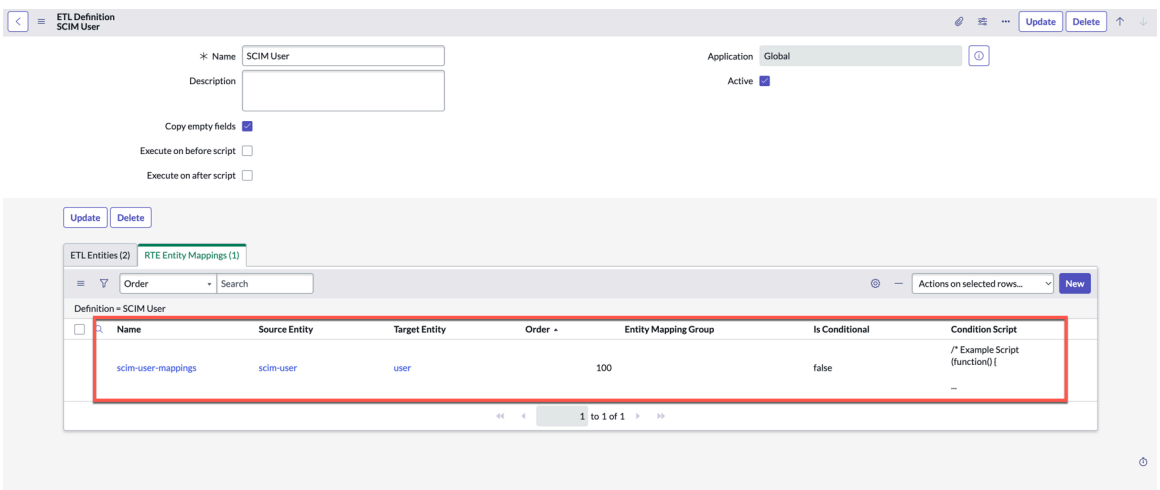
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Entité cible	Entité cible pour le mappage.
Ordre	Ordre dans lequel le mappage doit être traité.
Est conditionnel	Option permettant de désigner le mappage comme conditionnel.
Script de condition	Script qui définit les conditions devant être remplies pour le mappage.
Application	Le périmètre de l'application pour cet enregistrement.
Définition	Entité ETL sélectionnée à laquelle ce mappage appartient.
Ignorer	Option permettant de désigner si ce mappage d'entité ETL doit être ignoré lors de l'exécution d'intégrations de données à l'aide de la transformation robuste des ensembles d'importations (RTE).



7. Cliquez sur **Envoyer**.

L'exemple suivant montre un enregistrement créé pour mapper à la fois les enregistrements d'entité SCIM-user et d'utilisateur.



8. Ouvrez l'enregistrement soumis (scim-user-mappings) et créez un mappage entre les enregistrements scim-user et l'entité ETL de l'utilisateur.

   a. Dans la section Mappages de champs RTE, cliquez sur **Nouveau**.

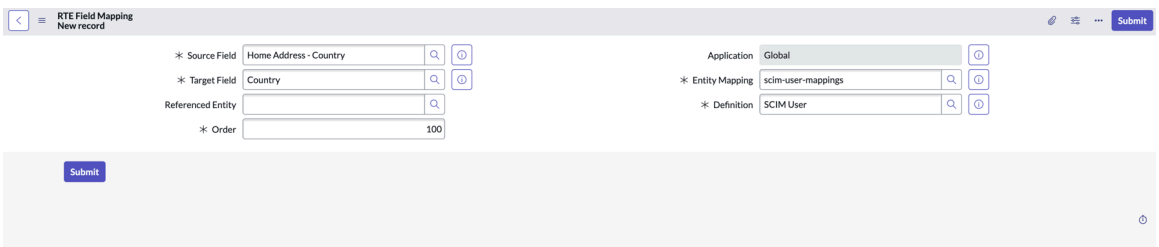
   b. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de l'entité ETL

Champ	Description
Champ source	Le périmètre de l'application pour cet enregistrement.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ cible	Champ ETL de sortie pour l'opération si l'opération prend une seule sortie.
Mappage d'entités	Mappage d'entités auquel cette opération s'applique.
Entité référencée	Entité référencée et opération à laquelle elle s'applique.
Définition	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Ordre	Ordre dans lequel l'opération s'exécute sur l'entité.



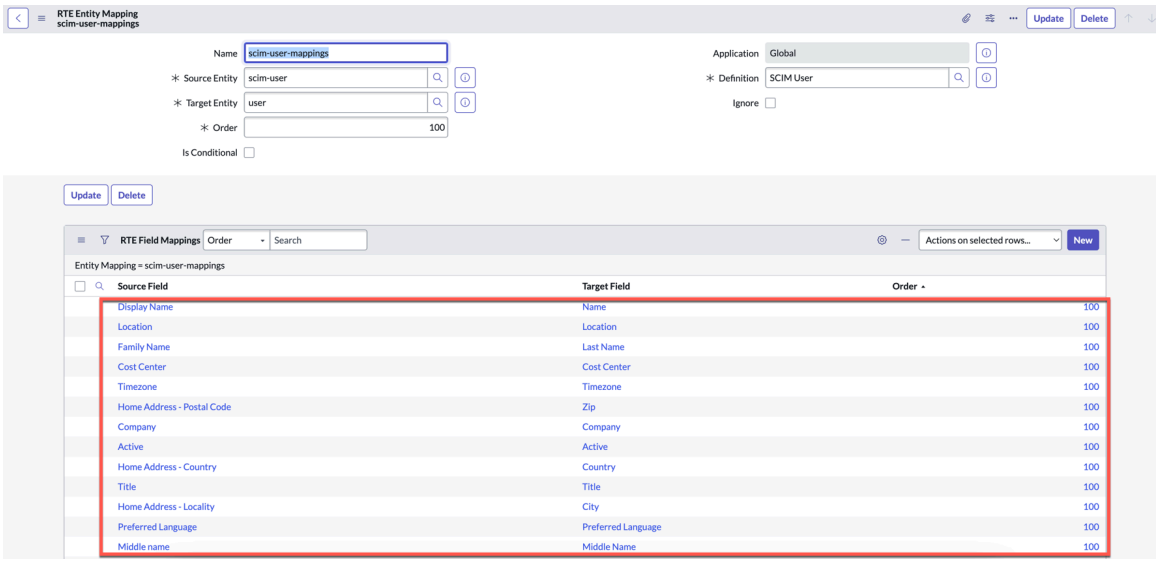
Le champ source **Adresse du domicile : pays** (entité ETL scim-user) mappe le champ cible en tant que **pays** (entité ETL utilisateur).

c. Soumettez les entrées en cliquant sur **Soumettre**.

Vous pouvez ajouter plusieurs entrées comme mappages d'entités RTE en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les champs sources et cibles sont mappés tels qu'ils sont configurés. Lorsque vous effectuez des opérations CRUD à l'aide de SCIM, les valeurs personnalisées sont mises à jour dans la table respective.

Résultats

Ces définitions et mappages ETL vous permettent d'extraire des données d'une table source, de transformer les données comme vous le souhaitez et de charger les données dans une table cible.

Information associée

Créer des définitions ETL (Extract Transform Load)

Gestion des champs non mappés

Vous pouvez gérer les champs non mappés dans la personnalisation SCIM de différentes manières.

Lors de la personnalisation SCIM, les champs qui ne font pas partie des tables sys_user et sys_user_group peuvent être mappés en exécutant les fonctions suivantes.

Personnaliser SCIM (créer ou mettre à jour)

Vous pouvez créer ou mettre à jour le client SCIM.

- L'administrateur SCIM peut ajouter des scripts personnalisés dans le et *`onAfter`* des *`onBefore`* scripts pour les champs qui ne sont pas mappés dans la définition ETL ou RTE.
- L'administrateur SCIM peut remplacer les mappages RTE en ajoutant des scripts personnalisés dans les *`onBefore`* scripts and *`onAfter`* .
- Vous pouvez appeler une API scriptable dans le ou les RTE *`onBefore`* pour *`onAfter`* accéder à la demande entrante et effectuer des transformations sur d'autres tables, listes et attributs non mappés.
- Vous pouvez utiliser la *`sn_auth.SCIM2Util.getScimProviderCustomizationContext()`* méthode pour fournir le contexte de demande SCIM qui contient l'objet *`scimResource`* . Le *`scimResource`* contexte dans représente les éléments suivants dans chaque opération :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **POST** : ressource SCIM envoyée dans la charge utile de la demande.
- **PUT** : ressource SCIM actuelle de la base de données remplacée par la ressource SCIM envoyée dans la charge utile de la demande.
- **PATCH** : ressource SCIM actuelle de la base de données après avoir effectué les opérations de correctif.

Voici un exemple de *`onAfter`* script.

```
(function onAfter(source, target, importLog) {

   var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
   gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

   var roles = ctx.scimResource.roles;
   if(roles) {
      var removingRolesGR = new GlideRecord("sys_user_has_role");
      removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
      removingRolesGR.query();
      removingRolesGR.deleteMultiple();

   for (var i = 0; i < roles.length; i++) {
      var addingRolesGR = new GlideRecord("sys_user_has_role");
      addingRolesGR.setValue("user", target.sys_user[0].sys_id);
      addingRolesGR.setValue("role", roles[i].value);
      addingRolesGR.setValue("state", "active");
      addingRolesGR.insert();
      }
      }
      var customUserExtn = new
 global.SCIMProviderCustomization().getCustomExtensionUrn('User');
      var salary = ctx.scimResource[customUserExtn].salary;
      if (salary) {
         var gr = new GlideRecord("u_user_salary");
         gr.addQuery("user", target.sys_user[0].sys_id);
         gr.query();
         if (gr.next()) {
            gr.setValue("salary", salary);
            gs.info("scim update: " + gr.update());
         } else {
         gr.setValue("salary", salary);
         gr.setValue("user", target.sys_user[0].sys_id);
         gr.insert();
         }
        }

})(source, target, importLog);
```

Personnaliser la réponse SCIM

Pour les appels d'API GET, toute réponse au client SCIM peut être personnalisée à l'aide du script en étendant le *`SCIMProviderCustomization`* script.

Lors de l'extension du script, l'auteur peut remplacer les *`customizeUserResponse`* méthodes et *`customizeGroupResponse`* pour modifier les réponses des ressources Utilisateur et Groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette *com.snc.integration.scim2.provider.customization.script.id* propriété permet au module d'extension SCIM d'utiliser le script qui doit être utilisé pour la personnalisation de la réponse.

Voici un exemple d'extension du script de base.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype = Object.extendsObject(SCIMProviderCustomization, {
   initialize: function() {
      SCIMProviderCustomization.prototype.initialize.call(this);
   },
   customizeUserResponse: function(context) {
      try {
         var rolesGR = new GlideRecord("sys_user_has_role");
         rolesGR.addQuery("user", context.scimResource.id);
         rolesGR.query();
         var i = 0;
         context.scimResource.roles = [];
         while (rolesGR.next()) {
            context.scimResource.roles[i] = {
               display: rolesGR.getElement('role.name').getValue(),
               value: rolesGR.getElement('role.sys_id').getValue()
            };
            i++;
         }
         var userGR = new GlideRecord("u_user_salary");
         userGR.addQuery("user", context.scimResource.id);
         userGR.query();
         if (userGR.next()) {
            var salary = userGR.getValue("salary");
            if (salary) {
               var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
context);
               customExtensionValue.salary = salary;
               SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this,
"User", context, customExtensionValue);
            }
         }
      } catch (ex) {
         gs.error("err: " + ex);
      }
      return context;
   },
   customizeGroupResponse: function(context) {
      return context;
   },
   type: 'SCIMCustomizationScript'
});
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le paramètre que contiennent les `customizeUserResponse` méthodes et `customizeGroupResponse` est un objet de contexte avec un attribut appelé `scimResource`. Cet attribut possède tous les attributs d'un objet de ressource d'utilisateur ou de groupe.
- Un include de script personnalisé ne peut être créé et consulté que par l'administrateur.
- Si une ressource utilisateur ou groupe est modifiée, vous devez rétablir le contexte.
- S'il n'y a aucune modification d'un attribut dans l'objet de ressource, définissez le `com.snc.integration.scim2.provider.customization.script.id` champ vide ou le renvoie comme nul.
- Si certains attributs sont conservés dans le `onAfter` script, ils doivent être renseignés avec des valeurs de base de données dans l'objet `scimResource` à l'intérieur du script personnalisé. Cette action est nécessaire pour que le système puisse effectuer les actions suivantes :
  - Pour obtenir le bon `scimResource` objet dans `onAfter` les scripts pendant l'opération PUT et PATCH.
  - Pour inclure les attributs qui ont persisté via le `onAfter` script dans la réponse au client.

Fonctions d'aide

Voici quelques-unes des fonctions d'aide pour la personnalisation SCIM. Ces fonctions vous permettent d'extraire ou de définir différents types d'informations.

Fonctions d'aide

Fonction	Objectif
`SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");`	Extraire l'extension de schéma personnalisé.
`SCIMProviderCustomization.prototype.getServiceNowExtensionUrn.call(this, "User");`	Obtenir la valeur d'extension de schéma ServiceNow .
`SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);`	Récupérer l'extension de schéma personnalisé dans la réponse.
`SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User", context);`	Récupérer l'extension de schéma ServiceNow dans la réponse
`SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);`	Définissez l'extension de schéma personnalisé dans la réponse.

Voici un exemple d'utilisation de la fonction d'assistance :

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue call(this, "User", context,
 customExtensionValue);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
RTE prend en charge la définition de données dans des tables autres que les tables sys_user et sys_user_group.

Création d'une définition de source

Créez une définition de source pour capturer des informations sur la source d'identité à partir de laquelle une ressource est mise en service.

Avant de commencer

Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, où l'scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Pourquoi et quand exécuter cette tâche

À l'aide d'une définition de source, la source d'identité de mise en service peut être mappée à une entité OAuth à l'aide de laquelle elle s'authentifie lors de la mise en service.

Une fois qu'une définition de source est créée, toutes les ressources mises en service à partir de cette source d'identité sont mappées à son ID de définition de source correspondant.

La définition de la source capture les informations sources requises, par exemple en procédant comme suit :

- Identifie le client SCIM à partir duquel la ressource est mise en service.
- Résout les informations en double fournies par l'ID externe :
  - Si plusieurs sources d'identité mettent en service des ressources, il peut y avoir deux ressources ou plus ayant la même valeur d'ID externe, car l'ID externe est uniquement unique à la source d'identité.
  - Si plusieurs ressources sont renvoyées avec un filtre SCIM d'ID externe, les ressources peuvent être résolues en fonction de la définition de source de la source d'identité demandeuse.

Remarque :
Une définition de source ne peut être créée que pour la source d'identité, qui utilise une méthode d'authentification OAuth.

Procédure

1. Accédez à la **Tous** > **SCIM** > **Définition de la source**.
2. Sur la page Définitions de source SCIM, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Définition de la source SCIM

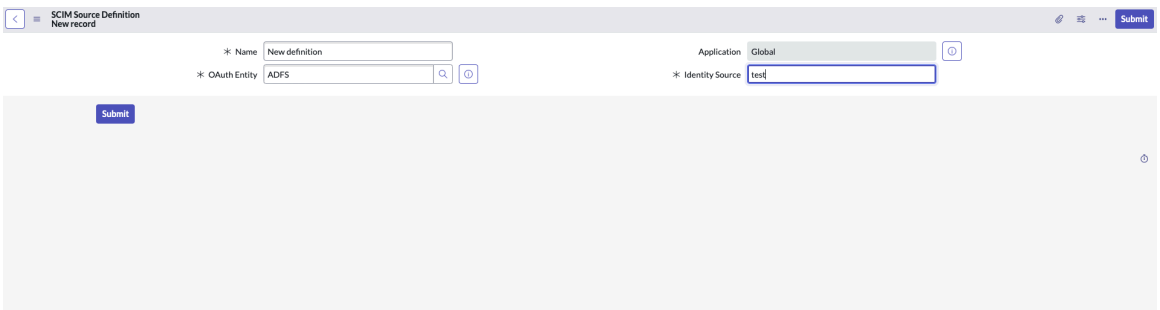
Champ	Description
Nom	Nom de la définition de la source.
Application	Le périmètre de l'application pour cet enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Entité OAuth	Entité OAuth de l'utilisateur d'intégration. L'entité est utilisée pour fournir l'utilisateur par le fournisseur de source d'identité.
Source d'identité	Le nom du fournisseur de source d'identité. Par exemple, Azure AD, Okta, etc

Remarque :
Activez la `com.snc.integration.scim2.resolve.externalid.conflict` propriété pour renvoyer uniquement les ressources SCIM créées par la source d'identité demandeuse. Par défaut, toutes les ressources correspondantes avec un filtre d'ID externe sont renvoyées.



4. Cliquez sur **Envoyer**.

Résultats
La définition de source SCIM est créée. Utilisez les définitions SCIM ETL pour mapper les ressources en fonction du schéma d'extension dans la table sys_user et sys_user_group. Pour plus d'informations, consultez Créer une définition SCIM ETL.

Client SCIM

Le client SCIM facilite le provisionnement et les mises à jour des ressources d'identité via des opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



En savoir plus sur SCIM Client.

Activer



Activez le client SCIM.

Propriétés du client SCIM



Obtenez des détails sur la personnalisation de SCIM.

Dépannage



En savoir plus sur la définition de source pour SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration du client SCIM

Le client SCIM facilite le provisionnement et les mises à jour des ressources d'identité via des opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

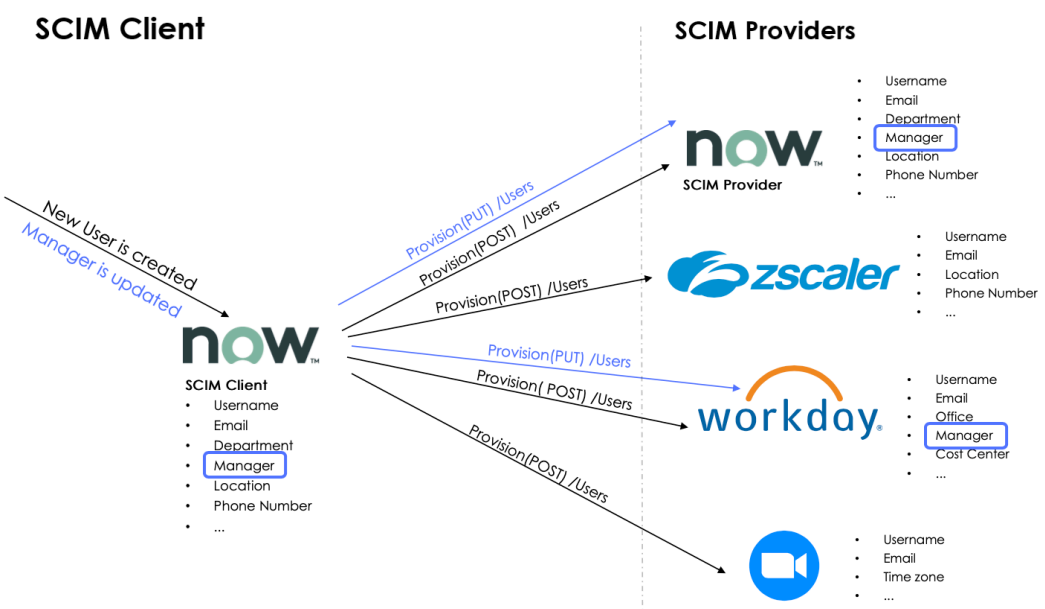
Le client SCIM est utilisé pour créer, mettre à jour et supprimer des ressources d'identité dans un système qui prend en charge les demandes REST compatibles SCIM. Le client est utilisé pour la gestion du cycle de vie des identités et pour la synchronisation des attributs d'identité entre les ServiceNow instances ou entre ServiceNow d'autres fournisseurs SCIM.

Étant donné que les API sont exposées par le client, vous pouvez automatiser le processus de création, de mise à jour ou de suppression de toutes les ressources sur un ou plusieurs fournisseurs SCIM. Par exemple, si un développeur rejoint l'organisation, vous devez lui donner accès à Git, à l'espace de travail, etc.

Le client SCIM vous permet d'effectuer les actions suivantes :

- Mettez en service les identités et les accès pour l'appartenance à un utilisateur ou à un groupe.
- Synchronisez les ressources d'identité et connexes avec les systèmes compatibles SCIM.
- Intégrez n'importe quel fournisseur SCIM sur ServiceNow®.
- Annuler la mise en service des identités et des accès.

Le client SCIM fournit des API scriptables que le développeur d'intégration peut utiliser pour créer des workflows ou des automatisations afin d'effectuer des tâches spécifiées. Pour en savoir plus sur l'API scriptable, consultez API SCIM2Client .



Configurations pour le client SCIM

Pour configurer le client SCIM, effectuez les tâches suivantes :

- Créez un message REST pour tous les appels sortants d'un fournisseur SCIM particulier. Pour plus d'informations, consultez Créer un message REST.
- Créez un fournisseur SCIM pour extraire les types de ressources et les informations de schémas du fournisseur SCIM avec le message REST. Activez la configuration de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

méthode HTTP (PUT OU PATCH) pour mettre à jour une ressource dans le fournisseur SCIM. Pour plus d'informations, consultez Créer un fournisseur SCIM.

- Créez les mappages des attributs SCIM aux attributs d'un type de ressource et d'un ServiceNow fournisseur SCIM particuliers. Pour en savoir plus, reportez-vous à la section Créer un mappage des ressources de fournisseur SCIM.
- Effectuez le mappage du champ SCIM avec la table de base de données et le nom du champ. Transmettez la valeur par défaut ou écrivez un script pour extraire la valeur. Pour plus d'informations, reportez-vous à la section Créer un mappage d'attribut SCIM.

Activer le module d'extension SCIM Client

Pour l'activation de SCIM Client, installez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée. Pour plus d'informations sur les composants installés avec un module d'extension, voir Rechercher les composants installés avec une application .

Propriétés, tables, API scriptables et journaux du client SCIM

Le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) inclut les propriétés système, les tables, les API scriptables et les journaux suivants.

Propriétés

Le client SCIM ajoute les propriétés système suivantes.

Propriétés

Nom	Description
com.snc.integration.scim2.client.log.request_state	Cette propriété détermine s'il faut écrire tous les enregistrements de journal ou uniquement les enregistrements du journal d'erreurs. Les valeurs possibles sont **FAILURE** ou **ALL.**

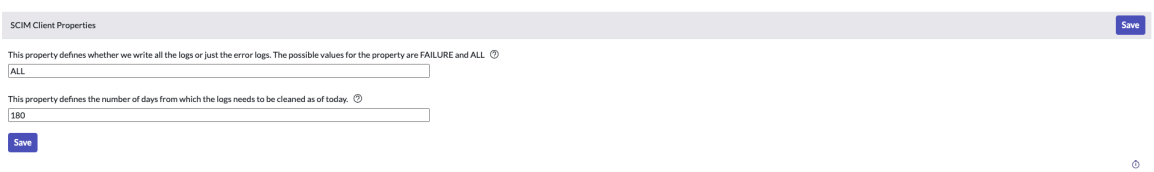
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
	Valeur par défaut : **TOUS**
com.snc.integration.scim2.client.log.cleanup.duration	Cette propriété détermine le nombre de jours pour effacer les journaux. Valeur par défaut : **180**

Pour définir les propriétés, accédez à **Tous** > **SCIM** > **Propriétés du client SCIM**.



Tables

Le client SCIM ajoute les tables suivantes.

Tables

Nom	Description
Fournisseur SCIM (sys_scim_provider)	Stocke les données de chaque fournisseur SCIM, telles que le nom, les définitions des ressources de message REST, etc.
Mappage des ressources de fournisseur SCIM (sys_scim_provider_resource_mapping)	Stocke les informations de table primaire pour chaque fournisseur et nom de ressource.
Mappage de l'attribut SCIM (sys_scim_attribute_mapping)	Stocke les détails de la source d'où chaque valeur d'attribut SCIM doit provenir, tels que le champ de table, le script, et ainsi de suite.
Journal client SCIM (sys_scim_client_logs)	Stocke les états de chaque appel déclenché vers le fournisseur SCIM.

Scriptable API

L'API SCIM2Client appelle le fournisseur SCIM (System for Cross-domain Identity Management) (rôle serveur) pour créer, mettre à jour ou supprimer des données dans un fournisseur de service (SP). L'API scriptable du client SCIM doit être utilisée dans les scripts en cours d'exécution dans le contexte système ou par un utilisateur administrateur système.

Par exemple, vous pouvez utiliser le script lors de l'exécution du workflow du concentrateur d'intégration en tant qu'utilisateur système, lors de l'exécution des travaux planifiés, etc.

Voici quelques-uns des cas d'utilisation de l'API scriptables :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- En tant qu'administrateur, fournissez des informations d'identité à partir de scripts en arrière-plan, de règles métier, d'appels d'include de script, de workflows, etc.
- En tant qu'administrateur, exécutez une tâche planifiée ou une tâche à la demande pour la mise en service d'identité.
- Exécutez un workflow ou un sous-workflow avec l'étape Script à l'aide de l'appel d'API pouvant contenir des scripts de mise en service.
- Ajoutez le script de mise en service directement dans une règle métier ou un script include. Le script peut être déclenché par des utilisateurs non-administrateurs. Ce cas d'utilisation fonctionne dans les situations suivantes :
  - L'utilisateur a accès au jeton, ce qui signifie qu'il a le rôle de générer le jeton à partir du modèle REST.
  - L'utilisateur peut récupérer les valeurs d'attributs SCIM à partir des tables mappées.

Pour en savoir plus sur l'API scriptable, consultez API SCIM2Client .

Journaux clients SCIM

Les journaux clients SCIM affichent l'état de mise en service des API SCIM. Pour afficher l'état de mise en service, accédez à **Tous** > **SCIM** > **Journaux clients SCIM**.

Créer un message REST

Configurez un message REST pour tous les appels sortants d'un fournisseur SCIM particulier.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Sortant** > **Message REST**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Fournisseur SCIM

Champ	Description
Nom	Nom descriptif pour ce message.
Point de terminaison	URL de base du fournisseur SCIM. Par exemple, https://example.service-now.com/api/now/scim.
Type d'authentification	Type d'authentification à utiliser pour se connecter au fournisseur SCIM externe. Pour plus d'informations, consultez Authentification REST sortante .
En-têtes de messages HTTP	Type de contenu attendu du fournisseur SCIM externe. Par exemple, le nom de l'en-tête est le type de contenu dans le corps de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	demande d'API suivant : Type de contenu : application/scim+json

4. Dans la liste connexe à Méthodes HTTP, cliquez sur **Nouveau**.
5. Configurez les méthodes HTTP suivantes.

Remarque :
Les URL contiennent des variables que vous devez remplacer.

Méthodes HTTP

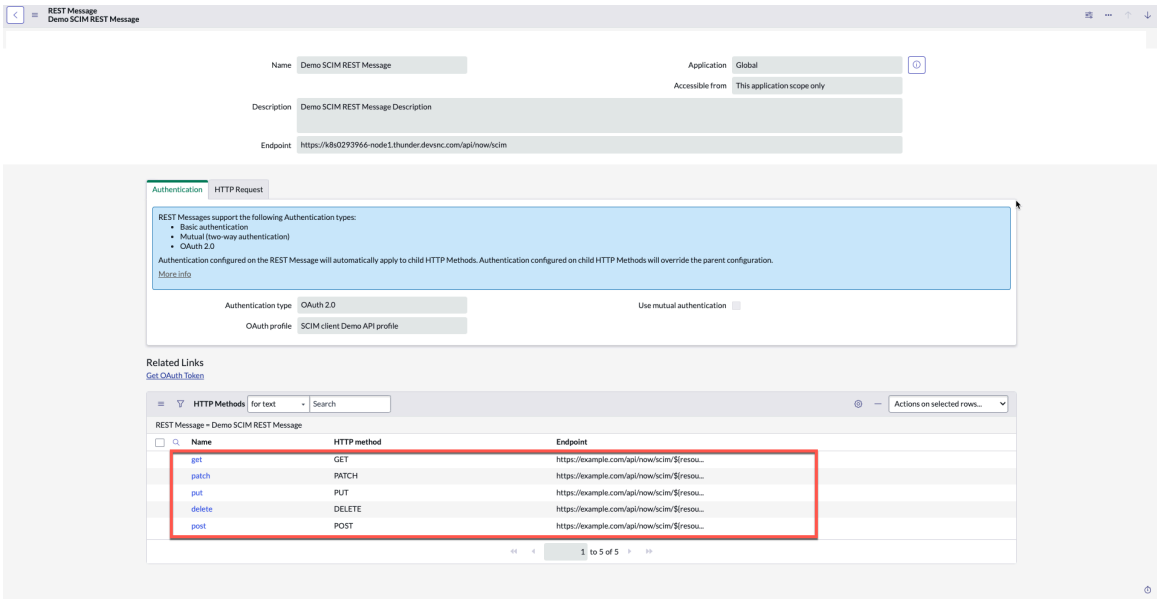
Méthodes	Exemple d'URL
GET	https://example.com/api/now/scim/${resourceName}
PATCH	https://example.com/api/now/scim/${resourceName}/${resourceId}
PUT	https://example.com/api/now/scim/${resourceName}/${resourceId}
DELETE	https://example.com/api/now/scim/${resourceName}/${resourceId}
POST	https://example.com/api/now/scim/${resourceName}/${resourceId}

Remarque :

- Vous devez créer toutes les méthodes HTTP pour le fonctionnement du client SCIM.
- Un exemple de message REST est envoyé à partir du système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Envoyer**.

Résultats
L'enregistrement du message REST est créé.

Que faire ensuite
Utilisez le message REST pour créer un fournisseur SCIM. Pour plus d'informations, consultez Créer un fournisseur SCIM.

Pour en savoir plus sur la création d'un message REST, consultez Créer un message REST .

Créer un fournisseur SCIM

Créez un fournisseur SCIM pour extraire les types de ressources et les informations de schémas du fournisseur SCIM avec le message REST. Activez la configuration de la méthode HTTP (PUT OU PATCH) pour mettre à jour une ressource dans le fournisseur SCIM.

Avant de commencer
Remarque :
Un exemple de fournisseur SCIM fait partie du système de base. Vous pouvez utiliser et configurer en fonction de vos besoins ou créer un nouvel enregistrement.

Rôles requis : admin

Procédure
1. Accédez à la **Tous** > **Client SCIM** > **Fournisseur SCIM**.
2. Sur la page Fournisseurs SCIM, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de fournisseur SCIM

Champ	Description
Nom	Nom du fournisseur SCIM

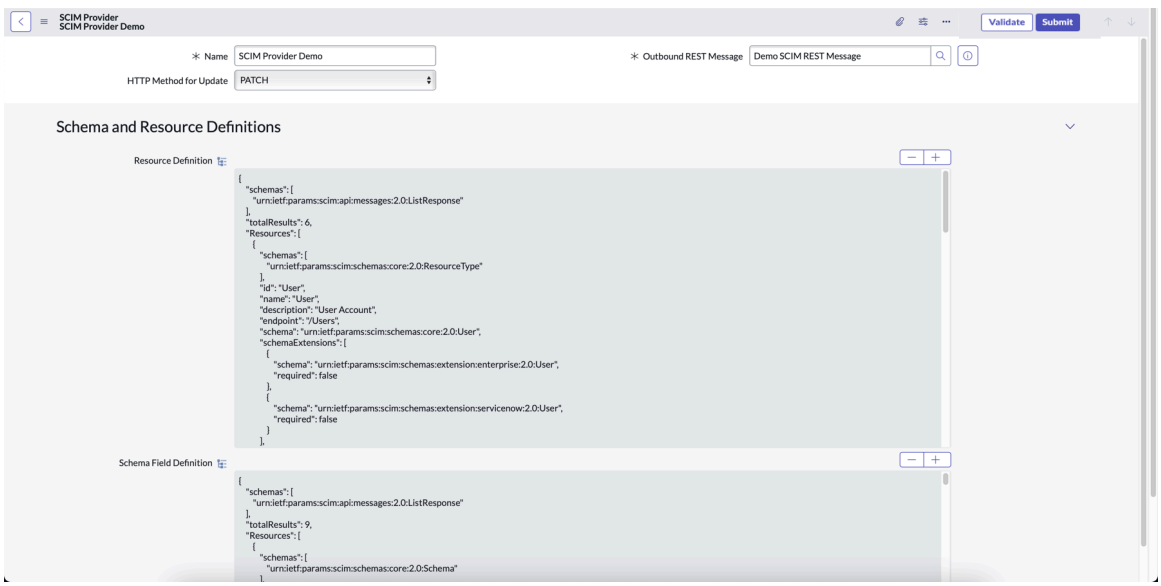
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Message REST sortant	Message utilisé pour appeler l'API du fournisseur SCIM. Pour plus d'informations, consultez Créer un message REST.
Méthode HTTP pour la mise à jour	Type de méthode HTTPS utilisé pour mettre à jour le mappage des ressources. La méthode PATCH ou PUT peut être utilisée par le client lors de la mise à jour de la ressource d'identité lors de la mise à disposition d'une ressource déjà existante.

Remarque :

- Les champs **Définition de la ressource** et **Définition du champ de schéma** sont récupérés à partir des points de terminaison publics du `/ResourceTypes` `/Schemas` fournisseur SCIM. Ces champs sont renseignés automatiquement une fois le message REST sélectionné.
- Si le message REST, les schémas ou les types de ressources sont mis à jour sur le fournisseur SCIM, cliquez sur **Actualiser** , puis sur **Mettre à jour** pour mettre à jour les champs **Définition de la ressource** et **Définition du champ de schéma** .



4. Cliquez sur **Envoyer**.

Résultats

Les détails du fournisseur SCIM sont créés avec succès. Utilisez le mappage des ressources de fournisseur SCIM pour mapper les détails du fournisseur SCIM aux ressources telles que les utilisateurs ou les groupes. Pour plus d'informations, consultez Créer un mappage des ressources de fournisseur SCIM.

Créer un mappage des ressources de fournisseur SCIM

Définissez les mappages des attributs SCIM aux attributs d'un type de ressource et d'un ServiceNow fournisseur SCIM particuliers.

Avant de commencer

Rôles requis : admin

Traduction automatique

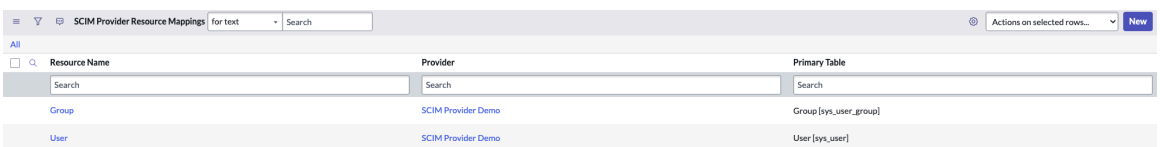
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Client SCIM** > **Mappage des ressources de fournisseur SCIM**.

   Le mappage des ressources de fournisseur SCIM est fourni avec le mappage d'utilisateur et de groupe par défaut.

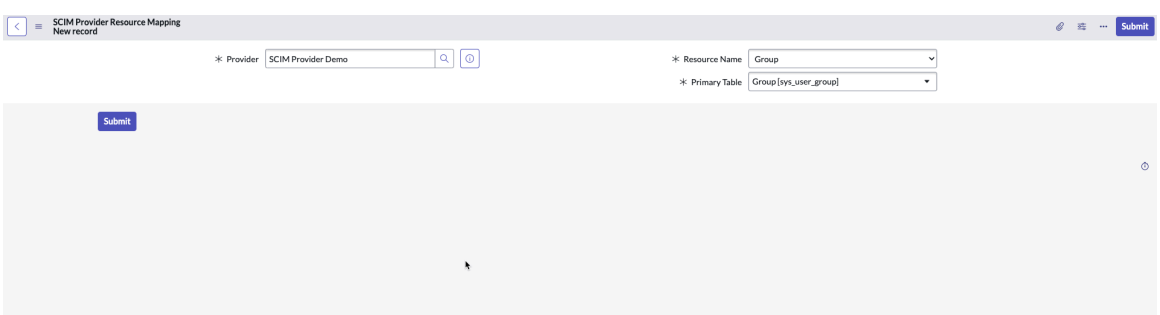
   Remarque :
   Les mappages d'utilisateur ou de groupe contiennent des exemples de mappages que vous pouvez utiliser comme référence. Vous pouvez également créer un mappage en fonction des ressources de l'utilisateur ou du groupe.



2. Créez un mappage de ressources en cliquant sur **Nouveau**.
3. Remplissez les champs du formulaire.

Mappage des ressources

Champs	Description
Fournisseur	Nom du fournisseur SCIM. Reportez-vous au nom du fournisseur configuré lors de la création d'un fournisseur SCIM.
Nom de la ressource	Ressource pour laquelle le mappage doit être défini.
Table primaire	Table qui contient le sys_id de la ressource en cours de mappage.



4. Cliquez sur **Envoyer**.

Résultats

L'enregistrement est créé et affiché dans la page Mappage des ressources de fournisseur SCIM. Utilisez les mappages d'attributs SCIM pour mapper davantage les attributs à partir de schémas. Pour plus d'informations, consultez Créer un mappage d'attribut SCIM.

Créer un mappage d'attribut SCIM

Créez un mappage d'attribut SCIM et utilisez-le comme source unique de ressource pour les champs de table ServiceNow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôles requis : admin

Pourquoi et quand exécuter cette tâche
Voici les types de mappage d'attributs et leurs descriptions.

Types de mappages d'attributs

Type de mappage d'attribut	Description
Direct	L'attribut SCIM est renseigné à l'aide des champs Nom de la **table de base de données** et **Nom du champ de base de données** .
Constante	L'attribut SCIM est renseigné à l'aide d'une valeur par défaut spécifiée.
Script/Personnalisé	L'attribut SCIM est renseigné à l'aide de la valeur de retour d'un script. Cet attribut nécessite l'activation de l'option Exécuter le script.

Remarque :

- L'attribut mot de passe n'est pas pris en charge
- Un exemple de mappage d'attributs pour les ressources Utilisateur et Groupe fait partie du système de base. Vous pouvez utiliser et configurer les mappages en fonction de vos besoins, ou vous pouvez créer un nouvel enregistrement.

Procédure

1. Accédez à la **Tous** > **Client SCIM** > **Mappage des ressources de fournisseur SCIM**.
2. A sélectionné le mappage de ressources SCIM créé pour la configuration.
3. Dans la liste connexe à Mappages d'attributs SCIM, cliquez sur **Nouveau**.



4. Remplissez les champs du formulaire.

Formulaire Mappages d'attributs SCIM

Champs	Description
Mappage des ressources de fournisseur	Mappage d'attribut pour une combinaison fournisseur-ressource.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	Si ce champ n'est pas renseigné automatiquement, utilisez l'option de recherche. Sélectionnez l'enregistrement Mappage des ressources du fournisseur.
Nom du schéma	Nom du schéma de l'attribut SCIM pour lequel le mappage doit être défini. Par exemple, *urn:ietf:params:scim:schemas:core:2.0:User*.
Attribut	Attribut pour lequel le mappage doit être défini. Par exemple, *userName*.
Sous-attribut	Sous-attribut (le cas échéant) pour lequel le mappage doit être défini. Par exemple, s'il existe un attribut de type complexe comme *name.familyName*, alors l'attribut est **name** et le sous-attribut est **familyName**.
Type de champ	Type de données Attribut SCIM. Ce champ est renseigné automatiquement à partir des schémas définis par le fournisseur SCIM. Par exemple, **booléen**.
Multivaleur	Plusieurs valeurs affectées à l'attribut. Un attribut peut avoir plusieurs valeurs comme e-mail professionnel, e-mail personnel ou un autre e-mail. Par exemple, *emails*. Ce champ est renseigné à l'aide des schémas définis par le fournisseur SCIM.
Condition de filtre	Certains attributs à valeurs multiples peuvent comporter des informations supplémentaires qui peuvent être spécifiées à l'aide d'une condition de filtre. Les choix de condition de filtre sont renseignés à l'aide des schémas définis par le fournisseur SCIM. Par exemple, l'attribut *phoneNumbers* a plusieurs types comme travail, mobile, maison, etc

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
Unique	Option permettant d'identifier de façon unique une ressource entre les systèmes Client SCIM et Fournisseur SCIM. Les attributs à valeurs multiples ne peuvent pas être marqués comme uniques. Par exemple, pour une ressource utilisateur, l'attribut *username* peut être rendu unique.
Nom de table de base de données	Utilisez ce champ pour mapper le nom de la table d'attributs au nom de la ServiceNow table. Si vous choisissez le mappage direct des attributs, vous devez définir ce champ. Par exemple, l'attribut *username* SCIM peut être mappé au champ **Utilisateur** du champ **Nom de table de base de données** .
Nom du champ de base de données	Le champ Nom du champ de base de données mappe l'attribut SCIM au ServiceNow nom de champ à mapper avec l'attribut SCIM. Si vous choisissez le mappage direct des attributs, vous devez définir ce champ. Par exemple, l'attribut *username* SCIM peut être mappé au champ **ID d'utilisateur** dans le champ **Nom du champ de base de données** .
Valeur par défaut	Détails sur la valeur par défaut transmise au fournisseur SCIM. Peut être utilisé sile mappage d'attribut direct du champ renvoie null, ou si la valeur par défaut peut être utilisée pour renvoyer une valeur codée en dur. Dans le cas d'une valeur codée en dur, le nom de la table de base de données et le nom du champ doivent être **Aucun**. Par exemple, la valeur du sous-attribut primaire de l'e-mail professionnel peut être codée en dur comme **vrai**.
Exécuter le script	Option permettant d'extraire la valeur de l'attribut via le script. Cette option est requise pour les attributs à valeurs multiples qui ne contiennent pas de condition de filtre. Pour un type

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	d'attribut complexe, un script peut fournir la valeur au niveau d'un attribut ou d'un sous-attribut. Par exemple, l'attribut **Membres** de la ressource de groupe n'a pas de condition de filtre. Ainsi, l'option de script doit être définie au niveau de l'attribut parent de l'attribut **Membres** .
Script	Script utilisé pour extraire la valeur de l'attribut. Le type de retour du script doit être une chaîne ou un JSON converti en chaîne. La sortie du script doit être au format approprié comme prévu par le fournisseur pour cet attribut.

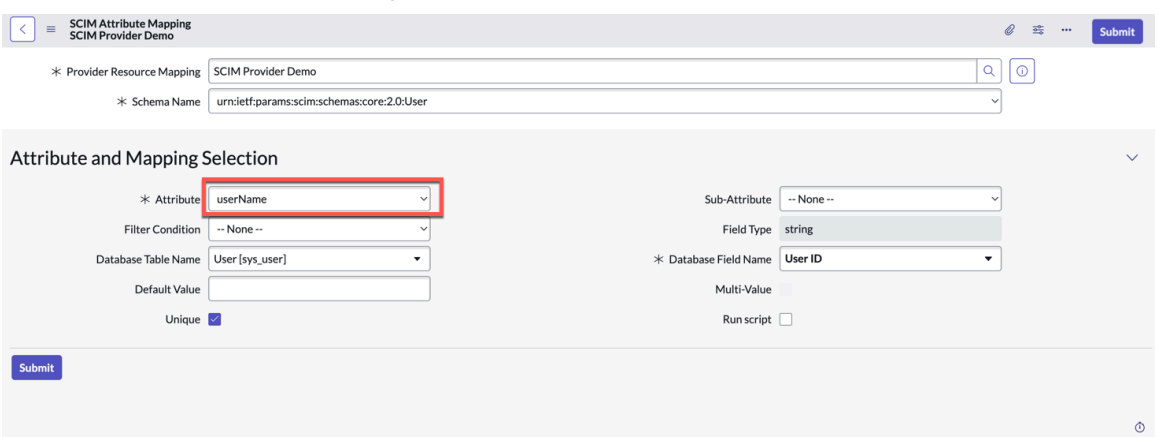
5. Cliquez sur **Envoyer**.

Références de mappage d'attribut

Les mappages d'attributs vous permettent d'utiliser les attributs comme une source unique de ressource pour les champs de table ServiceNow .

Attribut

Attribut pour lequel le mappage doit être défini. Par exemple, *`userName`*.



Sous-attribut

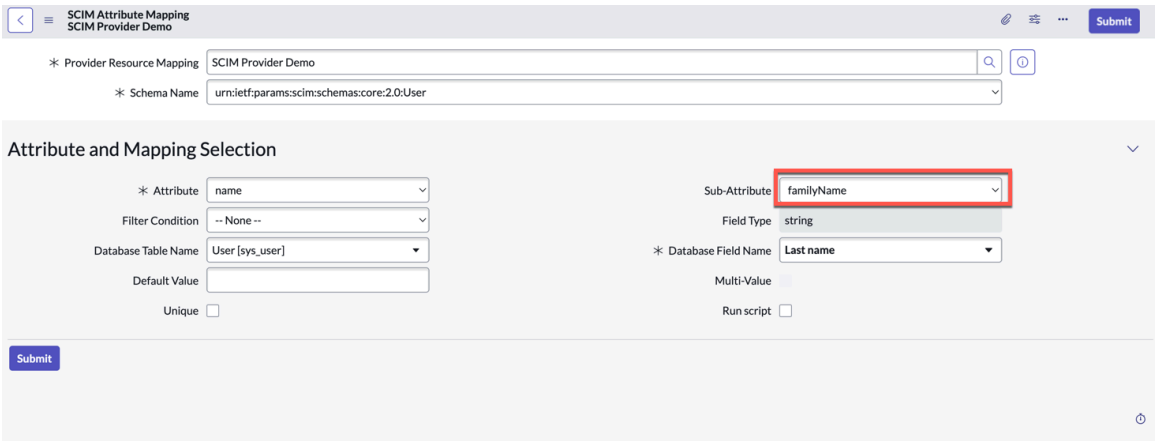
Sélectionnez le sous-attribut, le cas échéant, pour lequel un mappage doit être défini.

Par exemple, s'il existe un attribut de type complexe comme *`name.familyName`*, alors l'attribut est *`name`* et le sous-attribut est *`familyName`*.

Pour les attributs simples comme le nom d'utilisateur, la valeur du **sous-attribut** serait **Aucun**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

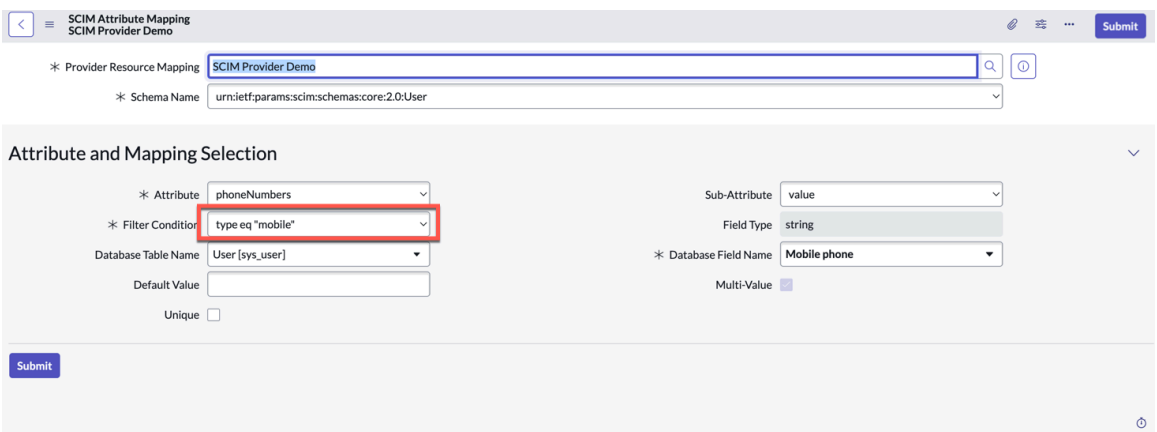


Condition de filtre

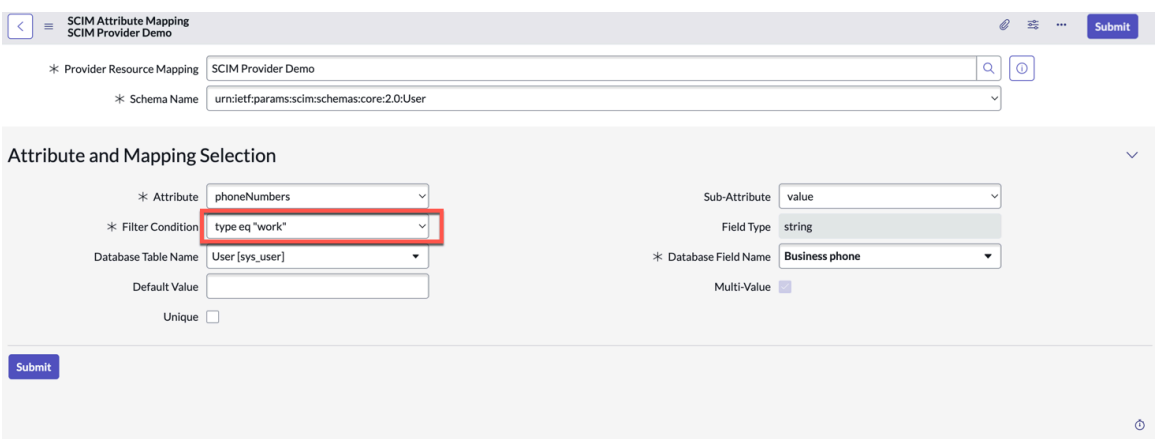
Un attribut à valeurs multiples peut contenir des informations supplémentaires qui peuvent être spécifiées à l'aide d'une condition de filtre. Les choix pour la condition de filtre sont renseignés à l'aide des schémas définis par le fournisseur SCIM.

Par exemple, l'attribut *phoneNumbers* a plusieurs types comme travail, mobile, domicile, etc.

Vous pouvez spécifier une condition de filtre parmi un ensemble de valeurs possibles. Par exemple, l'attribut *phoneNumber* peut avoir une condition de filtre **de type eq « mobile ».**



L'attribut *phoneNumber* peut avoir une condition de filtre de **type eq « work ».**



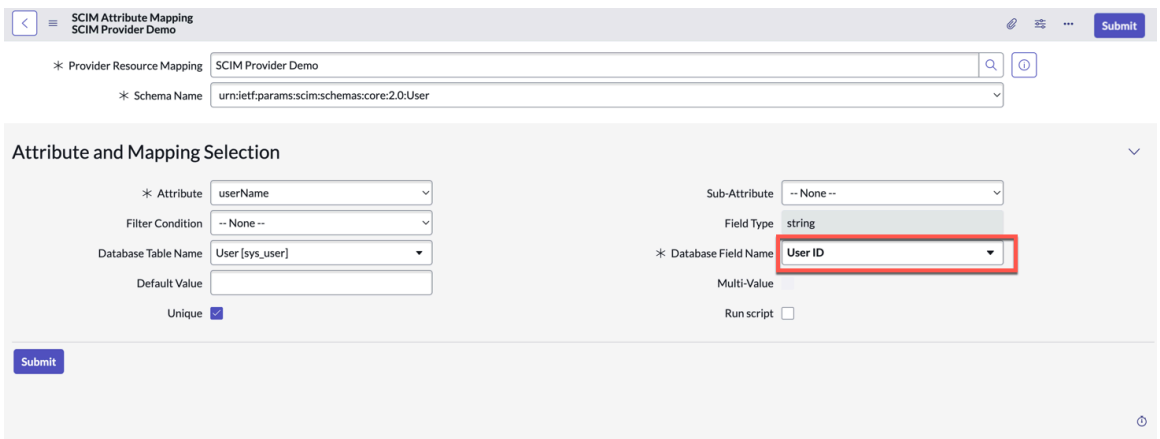
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

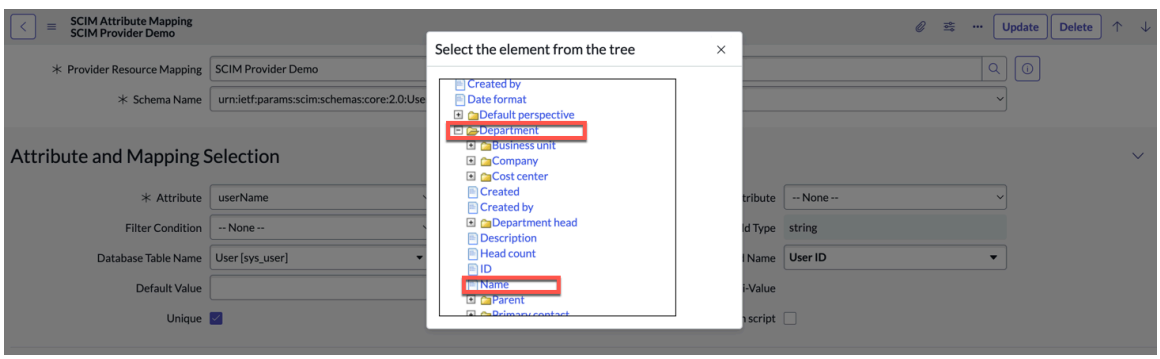
Nom du champ de base de données

Si l'option de mappage d'attribut direct est choisie, cet attribut doit être défini. Le champ **Nom du champ de base de données** représente le nom de ServiceNow champ mappé avec l'attribut SCIM.

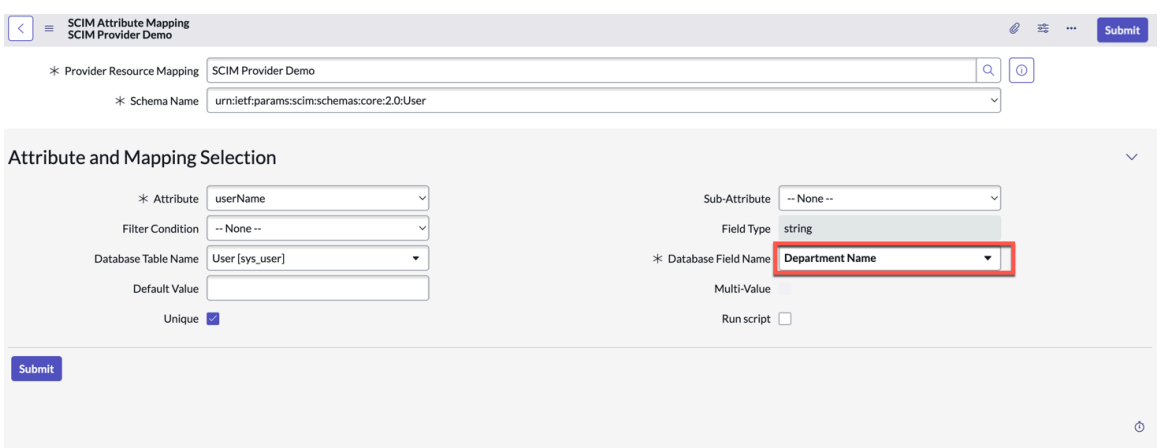
Par exemple, l'attribut *username* SCIM peut être mappé à un utilisateur en tant que champ Nom de table **de base de données** et au champ ID utilisateur en tant que champ **Nom du champ de base de données** .



Vous pouvez également effectuer une remontée pas à pas à l'aide du **nom du champ de base de données**. Par exemple, l'attribut SCIM du **département** peut être mappé au champ **Nom du département** .



Ici, la table de base de données est **Utilisateur** et le nom du champ Base de données est **Nom du département**.



Traduction automatique

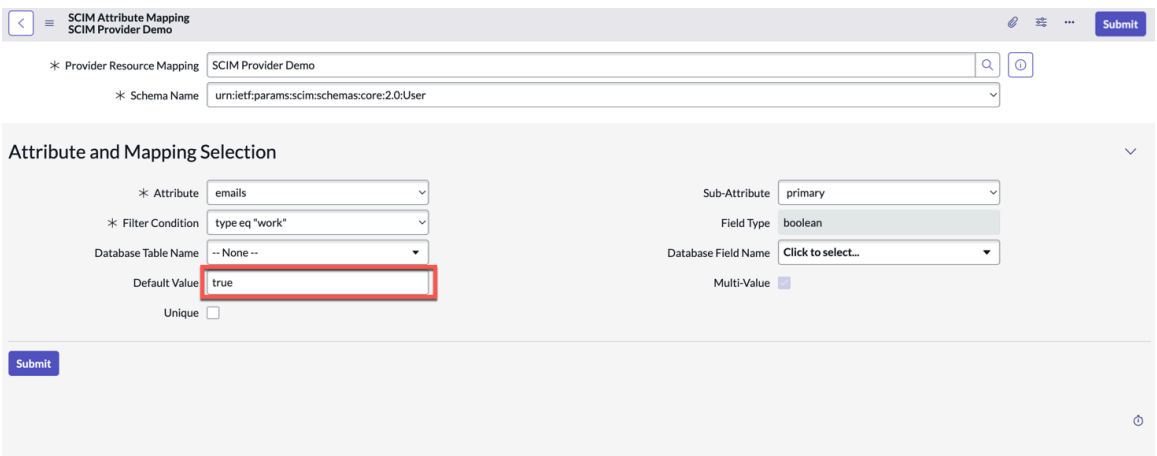
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur par défaut

La valeur par défaut est transmise au fournisseur SCIM si le mappage d'attribut direct de ce champ renvoie une valeur null. La valeur par défaut peut également être utilisée pour renvoyer une valeur codée en dur.

Dans le cas d'une valeur codée en dur, le nom de la table de base de données et le nom du champ doivent être **Aucun**.

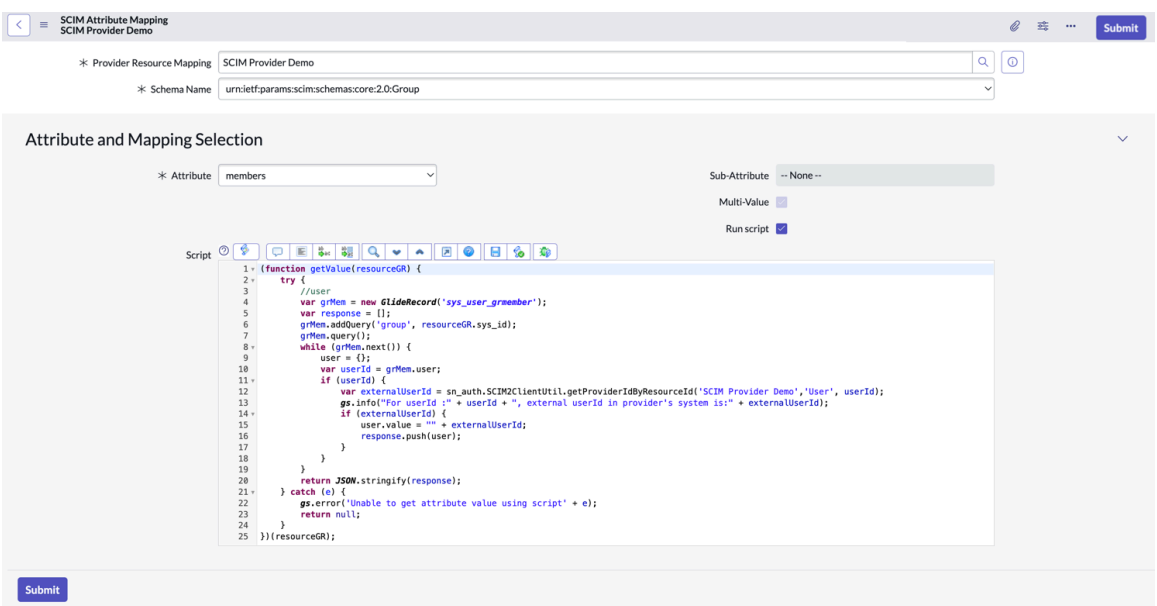
Par exemple, la valeur du sous-attribut primaire de l'e-mail professionnel peut être codée en dur comme **vrai**.



Script

Le script est utilisé pour extraire la valeur de l'attribut. Le type de retour du script doit toujours être une chaîne de caractères, ou un JSON converti en chaîne. La sortie du script doit être au format approprié comme prévu par le fournisseur pour cet attribut.

Voici un exemple de script pour un attribut à valeurs multiples.

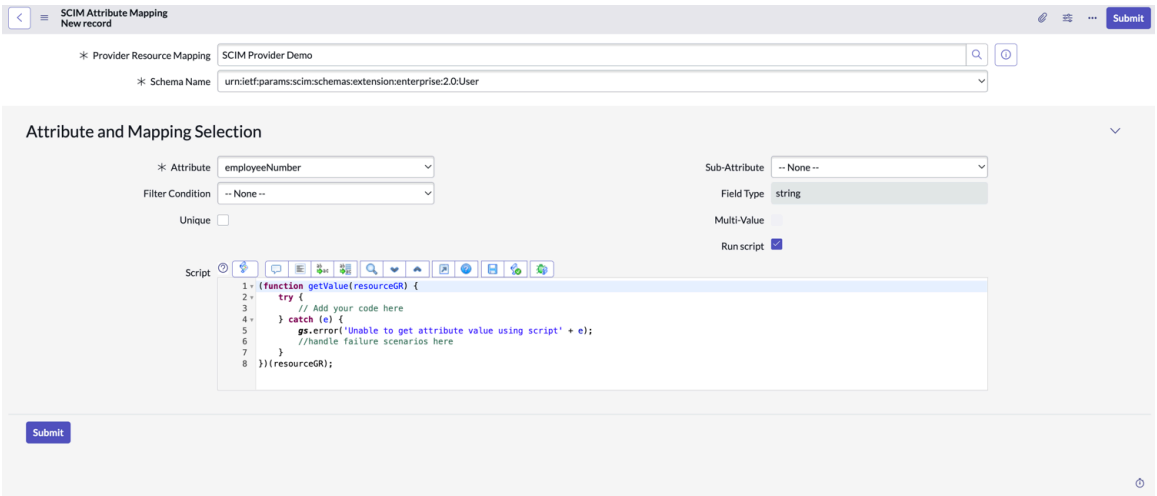


La sortie du script doit avoir un tableau JSON stringified.

Voici un exemple de script d'un attribut à valeur simple.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La sortie du script doit être une chaîne.

Dépannage du client SCIM

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de la configuration ou de l'exécution du client SCIM.

Dépannage

Problème	Action
La réponse contient le message suivant : `"message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	Le message s'affiche si l'API est appelée dans un contexte utilisateur et que l'utilisateur n'a pas accès à la table. Vous devez vous assurer que l'API scriptable est appelée dans le contexte du système.
La réponse contient le message suivant : `{"message":"User Not Authenticated","detail":" Required to provide Auth information"}`	• Assurez-vous que le jeton est généré via le message REST correspondant et qu'il est valide. • Assurez-vous que l'API scriptable est appelée dans le contexte du système.
La réponse contient le message suivant : `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	Dans le mappage d'attributs SCIM, si le champ est défini pour être récupéré à partir d'un script présentant ce problème, assurez-vous que le type de retour doit toujours être une chaîne.
La réponse contient le message suivant : `"status": "400", "scimType": "invalidValue",`	Pour tout attribut SCIM qui attend l'ID, cet ID est toujours celui du système du fournisseur. Assurez-vous que l'ID transmis dans la charge utile est valide dans le système du fournisseur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Problème	Action
"detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"	

Domaines à vérifier pour le dépannage

Voici quelques-unes des zones qui peuvent être vérifiées pour les erreurs de résolution lors de l'utilisation du client SCIM :

- Si un problème est détecté lors de l'exécution de l'une des API scriptables, consultez la section Journaux clients SCIM.

Champs de journaux

Champ	Description
ID de demande	ID unique qui représente une API pouvant contenir un script appelée.
Fournisseur SCIM	Nom du fournisseur pour lequel l'API est appelée.
Ressource	Nom de la ressource pour laquelle l'API est appelée.
ID de ressource	ID pour lequel l'API est appelée. Pour la suppression, l'ID représente l'ID de ressource dans le système du fournisseur et l'ID se trouve dans le système client.
Action	API appelée
Statut	État du journal en tant que réussite ou échec
Message	Message de réussite ou d'erreur. Le message d'erreur peut provenir du fournisseur SCIM ou de problèmes de configuration dans le client SCIM.

- Vérifiez le corps de la demande en configurant et en visualisant les appels sortants. Pour en savoir plus, consultez Journalisation des services Web sortants .
- Mettez à jour les niveaux de journal en ajoutant le type de contenu, en testant l'exemple et en accédant au formulaire de méthode HTTP correspondant dans le message REST du fournisseur correspondant.
- Si le corps de la demande est tronqué, augmentez la limite à l'aide de la propriété `glide.outbound_http.content.max_limit`système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

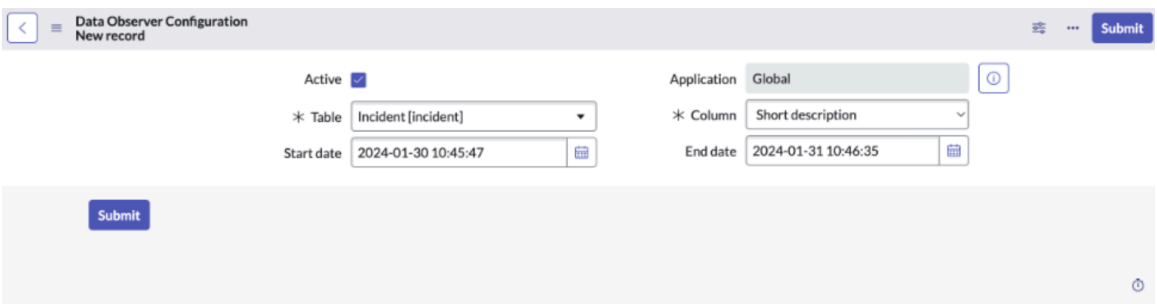
Observateur d'accès

Utilisez Observateur d'accès pour comprendre les données d'accès des personnes et des processus sur votre instance.

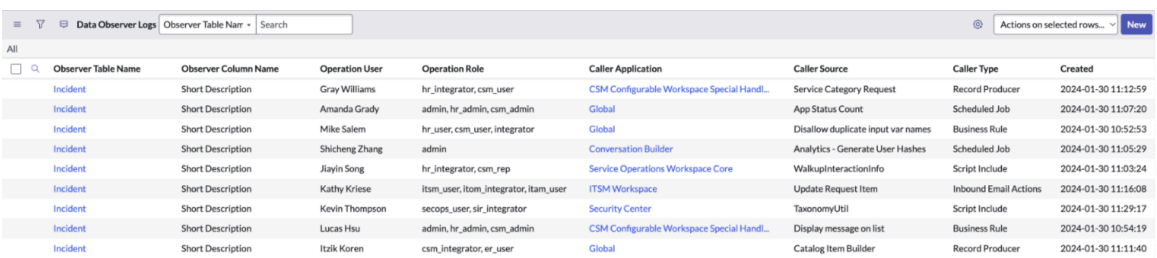
Avec Access Observer, les administrateurs de sécurité peuvent :

- Identifiez les entités telles que les utilisateurs, les rôles, les applications incluses dans le périmètre et les scripts qui accèdent à vos données.
- Utilisez cette connaissance préalable pour savoir comment appliquer au mieux la sécurité afin de limiter les accès inutiles à vos données, tout en confirmant celles qui nécessitent un accès et qui fonctionnent toujours normalement.
- Évitez les pannes d'automatisation en ayant une vue claire de la façon dont l'accès à vos données est possible avant d'apporter des modifications de sécurité.
- Répondez au besoin de fournir des informations sur la manière dont le chiffrement est appliqué sur votre instance.

Configurez l'Observateur d'accès en créant des enregistrements de configuration d'Observateur d'accès. Dans ces enregistrements, vous définissez une table et une colonne spécifiques à observer et l'heure à laquelle la colonne est observée.



Trouvez les résultats de vos observations sur la table d'enregistrement du journal Access Observer. Sur cette table, vous pouvez voir un enregistrement détaillant chaque accès à la colonne spécifiée.



Observer Table Name	Observer Column Name	Operation User	Operation Role	Caller Application	Caller Source	Caller Type	Created
Incident	Short Description	Gray Williams	hr_integrator, csm_user	CSM Configurable Workspace Special Handl...	Service Category Request	Record Producer	2024-01-30 11:12:59
Incident	Short Description	Amanda Grady	admin, hr_admin, csm_admin	Global	App Status Count	Scheduled Job	2024-01-30 11:07:20
Incident	Short Description	Mike Salem	hr_user, csm_user, integrator	Global	Disallow duplicate input var names	Business Rule	2024-01-30 10:52:53
Incident	Short Description	Shicheng Zhang	admin	Conversation Builder	Analytics - Generate User Hashes	Scheduled Job	2024-01-30 11:05:29
Incident	Short Description	Jiayin Song	hr_integrator, csm_rep	Service Operations Workspace Core	WalkupInteractionInfo	Script Include	2024-01-30 11:03:24
Incident	Short Description	Kathy Kriese	itsm_user, itom_integrator, itam_user	ITSM Workspace	Update Request Item	Inbound Email Actions	2024-01-30 11:16:08
Incident	Short Description	Kevin Thompson	secops_user, sir_integrator	Security Center	TaxonomyUtil	Script Include	2024-01-30 11:29:17
Incident	Short Description	Lucas Hsu	admin, hr_admin, csm_admin	CSM Configurable Workspace Special Handl...	Display message on list	Business Rule	2024-01-30 10:54:19
Incident	Short Description	Itzik Koren	csm_integrator, er_user	Global	Catalog Item Builder	Record Producer	2024-01-30 11:11:40

Configurer l'observation relative à l'accès

Créez un enregistrement d'observation d'accès pour examiner l'accès à une colonne de données pendant une fenêtre de temps spécifiée.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Observateur d'accès** > **Configuration de l'Observateur d'accès**.
2. Sélectionnez **Nouveau** pour créer un enregistrement.
3. Remplissez les champs du formulaire.

Champs de configuration de l'Observateur d'accès

Champ	Description
Actif	Indique si l'enregistrement est actif ou non. Votre enregistrement est automatiquement marqué comme actif pendant la période d'observation et est inactif dans les autres cas.
Application	L'application incluse dans le périmètre de l'enregistrement. Ce champ est en lecture seule.
Table	Table qui contient la colonne à observer
Colonne	Colonne de la table sélectionnée à observer.
Démarrer la tâche immédiatement	Si cette option est sélectionnée, l'observation commence dès la création de l'enregistrement.
Date et heure de fin	Heure à laquelle l'observation prend fin.
Date/heure de début	Heure à laquelle l'observation commence. Ce champ n'est visible que si **l'option Démarrer la tâche immédiatement** n'est pas sélectionnée.

4. Sélectionnez **Soumettre** pour sauvegarder l'enregistrement.

Que faire ensuite

Une fois la fenêtre d'observation que vous avez définie démarrée, vous pouvez voir chaque instance à laquelle la colonne a été accédé détaillée dans les enregistrements de la table Journal d'observateur d'accès [sys_data_ob_log].

Examiner les journaux de l'Observateur d'accès

Utilisez les informations contenues dans les enregistrements du journal de l'observateur d'accès pour obtenir un aperçu de la façon dont vos données sont accessibles.

Une fois que vous avez configuré un ou plusieurs enregistrements d'observation d'accès, votre instance commence à créer des enregistrements de journal d'observateur d'accès avec des détails sur l'accès aux colonnes que vous avez choisies. Vous pouvez trouver ces enregistrements sur votre instance à l'adresse **Tous** > **Observateur d'accès** > **Journal de l'Observateur d'accès**.

Résultats du journal de l'Observateur d'accès

Utilisez la table suivante pour comprendre les informations présentées dans les journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de journal de l'observateur d'accès

Champ	Description
Nom de la table de l'observateur	La table sélectionnée dans l'enregistrement d'observation d'accès qui a généré cet enregistrement.
Nom de la colonne Observateur	Colonne sélectionnée dans l'enregistrement d'observation d'accès qui a généré cet enregistrement.
Utilisateur de l'opération	Utilisateur ayant accédé à la colonne
Rôle de l'opération	Rôles de l'utilisateur qui a accédé à la colonne
Application de l'appelant	L'application incluse dans le périmètre à partir de laquelle l'accès aux données a été effectué.
Type d'appelant	Type d'élément ayant accédé à la colonne, tel que créateur d'enregistrement, tâche planifiée ou règle métier.
ID de document de la source de l'appelant.	
Source de l'appelant	Élément ayant accédé à la colonne. Utilisé avec le champ **Type d'appelant** pour voir ce qui a spécifiquement accédé à la colonne. Par exemple, si le type d'appelant est `Règle métier`, la source de l'appelant est le nom de la règle métier qui a accédé à la colonne.
Hachage primaire	
Nombre de répétitions	
Pile Java	
Pile JavaScript	
ID de session	ID de la session dans laquelle la colonne a été consultée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ressources supplémentaires pour les produits et solutions Platform Security

Si vous recherchez les bonnes pratiques de sécurité de la plateforme, le dépannage ou d'autres directives d'implémentation, sélectionnez une fonctionnalité ou un type de ressource pour découvrir ServiceNow des ressources sur d'autres sites web pertinents.

Remarque :
De nombreuses ressources de cette table nécessitent que vous vous connectiez à des sites tels que ServiceNow Université, Now Create ou la ServiceNow communauté. Si la ressource attendue ne se charge pas, veuillez vous connecter et essayer d'accéder à nouveau à la ressource.

Liens de ressources

Fonctionnalités ou produits de sécurité de la plateforme	Type de ressource	Ressources
Centre de sécurité	Mise en route	Centre de sécurité ServiceNow
Centre de sécurité	Bonnes pratiques	• Bonnes pratiques : Centre de sécurité • Bonnes pratiques de sécurisation renforcée du centre de sécurité
Centre de sécurité	Questions fréquentes	Sécurisation renforcée de la sécurité ServiceNow : Centre de sécurité
Signature de code	Mise en route	• Signature de code pour une défense en profondeur améliorée • Signature de code et cercle de confiance (CoT) : introduction
Confidentialité des données	Conseils et exemples	[Communiqué de Washington] Atténuation du risque d'exposition involontaire des données sensibles grâce à Confidentialité des données
Chiffrement de champ	Conseils et exemples	Chiffrement au niveau du champ dans ServiceNow
Chiffrement de champ Enterprise	Mise en route	Différences entre le chiffrement au niveau du champ et le chiffrement au niveau de la plateforme
Chiffrement de champ	Dépannage	• Pourquoi le chiffrement au niveau du champ n'est-il pas appliqué aux champs du type de données Numéro de téléphone ? • Nous chiffrons le niveau de champ sur le ticket Relations avec les employés • Chiffrement des pièces jointes à l'aide de « Chiffrement au niveau du champ » • Impossible de supprimer une configuration de champs chiffrés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens de ressources (suite)

Fonctionnalités ou produits de sécurité de la plateforme	Type de ressource	Ressources
		• La table de ticket n'est pas disponible dans la configuration de champ chiffré • L'interrogation du champ chiffré ne renvoie pas de résultats cohérents dans les travaux planifiés
Chiffrement de champ Enterprise	Dépannage	• Chiffrement au niveau du champ Enterprise : configuration initiale • Field Level Encryption Enterprise : limites et considérations • Chiffrement au niveau du champ Enterprise : administration
Chiffrement Edge	Dépannage	• Vue d'ensemble de Chiffrement Edge sur ServiceNow • Chiffrement Edge : configuration initiale • Règles Chiffrement Edge • Chiffrement Edge : limites • Chiffrement Edge : administration
Chiffrement Edge	Conseils et exemples	• Ressources Chiffrement Edge • Journaux du proxy Chiffrement Edge • Notification d'expiration du certificat Chiffrement Edge
Chiffrement Edge	Dépannage	• Graphiques des performances de chiffrement Edge • Chiffrement Edge étend la longueur du champ
Chiffrement de la base de données	Conseils et exemples	Chiffrement de la base de données dans ServiceNow : TSE/DBE à l'aide de CCS
Gestion des accès	Conseils et exemples	Gestion des identités et des accès avec ServiceNow
Accès zéro confiance	Dépannage	Aide avec l'analyseur d'accès, l'accès zéro confiance et l'authentification adaptative sur ServiceNow
Séparation en domaines pour les fournisseurs de services	Dépannage	Séparation de domaine ServiceNow pour les fournisseurs de services
Filtration des données	Mise en route	Comprendre le module d'extension « Filtrage des données »
Rôles de sécurité	Conseils et exemples	Comment fonctionnent les rôles de sécurité ?

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens de ressources (suite)

Fonctionnalités ou produits de sécurité de la plateforme	Type de ressource	Ressources
Connexions et informations d'identification	Mise en route	Vue d’ensemble des connexions et des informations d’identification : découvrir les intégrations sur le ServiceNow AI Platform
ServiceNow Contrôles d’accès	Conseils et exemples	Contrôles d’accès - La méthode la plus simple
Centre de sécurité	Bonnes pratiques	Bonnes pratiques : Centre de sécurité
Sécurité de la plateforme	Bonnes pratiques	• Guide des bonnes pratiques de sécurité ServiceNow • Sécurisation de la plateforme d’IA ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.